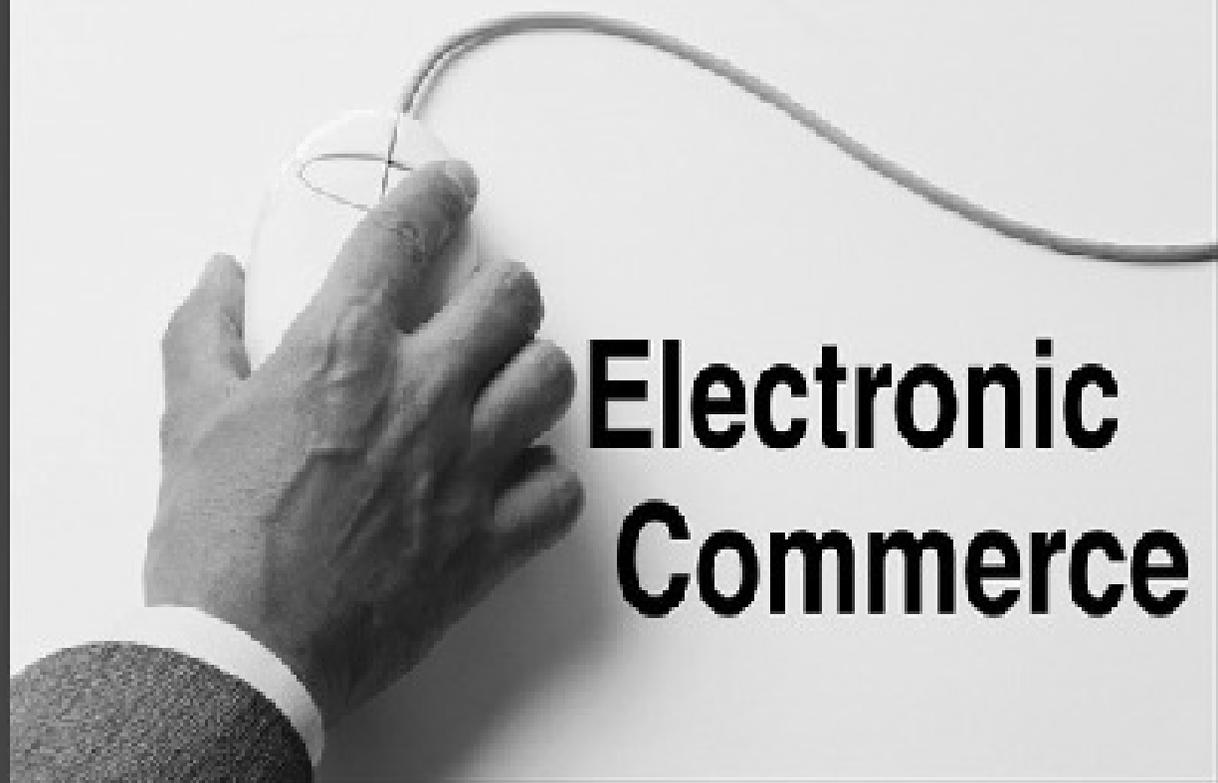
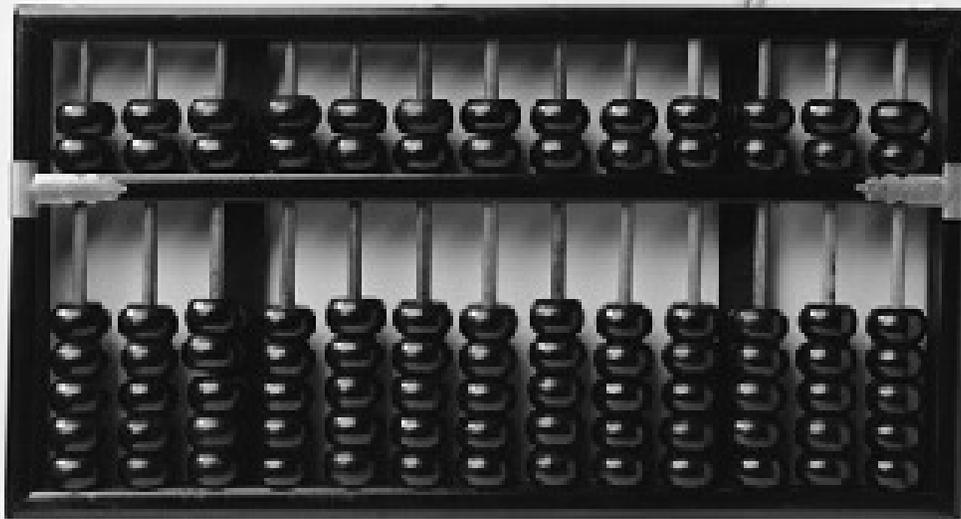


g l o b a l i s s u e s

O c t o b e r 1 9 9 7 V o l u m e 2 N u m b e r 4



Electronic Commerce



We cannot imagine exactly what the 21st century will look like, but we know that its science and technology and its unprecedented fusions of cultures and economies will be shaped in large measure by the Internet.

One of the most revolutionary uses of the Internet is in the world of commerce. Already, we can buy books and clothing, obtain business advice, purchase everything from garden tools to hot sauce to high-tech communications equipment over the Internet. But we know it is just the beginning. Trade on the Internet is doubling or tripling every single year. In just a few years, it will generate hundreds of billions of dollars in goods and services.

If we establish an environment in which electronic commerce can grow and flourish, then every computer will be a window open to every business, large and small, everywhere in the world.

President Bill Clinton

global issues

An Electronic Journal of the U.S. Information Agency
Volume 2, Number 4 October 1997



table of contents

ELECTRONIC COMMERCE

focus

A Market for Just About Anything	6
With electronic commerce people will have a virtual shopping mall that is always open all across the world. Excerpts of remarks by Vice President Al Gore.	
Cooperation Needed	8
Electronic commerce will rely upon private sector solutions and market-driven possibilities. It will not be, and should not be, a government-run marketplace. Excerpts of remarks by Secretary of Commerce William Daley.	
Global Partnership For E-Commerce	11
The U.S. government is working with other governments and the world business community to create a digital economy. An interview with Ira Magaziner, senior advisor to President Clinton for policy development.	

commentary

New Products, Services Needed	14
The challenge is to develop products and services that are more than just digitalized versions of traditional business. An interview with Internet pioneer-developer Vinton Cerf.	
The Internet Has Come of Age	17
The Internet is not only open for business, it is ready for business. Excerpts of remarks by Louis V. Gerstner, Jr., chairman and chief executive officer of IBM Corporation.	
Keep Big Brother's Hands Off the Internet	19
If Internet users are to truly benefit from the new means of commerce, communication, and education that technology offers, governments should avoid harnessing the Internet with a confusing array of intrusive regulations and controls. <i>By Senator John Ashcroft, Republican, Missouri</i>	

The Risks and Rewards	22
Businesses need to understand the changes the information age offers and take advantage of them. <i>By Larry Irving, Assistant Secretary of Commerce for Communications and Information</i>	
Securities Fraud Looms as Dark Side of Internet Growth	25
The dramatic growth in online investing has a dark side to it — criminals looking for opportunities to defraud unsuspecting investors. <i>By Jim Fuller</i>	
The Internet and Global Trade	28
With the Internet, our communication distance has diminished to near zero, fostering long-distance relationships that become apparent immediately to every hopeful entrepreneur who establishes a Website. <i>By Harold Wolhandler, Director of Research, ActioMedia, Inc.</i>	

reports and documents

A Framework for Global Electronic Commerce	33
This executive summary of a White House report sets forth general principles for a world-wide, free-trade zone on the Internet.	
Electronic Cash and the End of National Markets	38
As the use of electronic cash soars, governments will face difficulties in controlling monetary policy, taxation, financial regulation, and crime. <i>By Stephen J. Kobrin</i>	

departments

Bibliography	45
Books, documents and articles on electric commerce	
Internet Sites	48
A list of Internet sites on electronic commerce issues	

Cover: Design from images. Copyright (c) 1996 PhotoDisc, Inc.

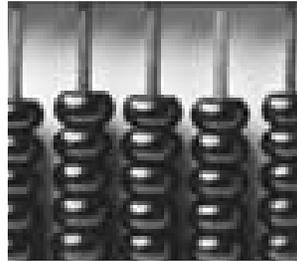
GLOBAL ISSUES

An Electronic Journal of the U.S. Information Agency
ejglobal@usia.gov

Publisher Judith S. Siegel
Editor John Walsh
Managing Editor Edmund F. Scherr
Text Editor Jim Fuller
Internet Editor Tim Brown
Associate Editors Guy Olson
..... Wayne Hall
Contributing Editors Jerry Stilkind
Reference and Research Monica Mieroszewska
..... Joan Taylor
Art Director Chloe Ellis
Graphics Assistant Sylvia Scott
Cover Design Barry Fitzgerald
Editorial Board Howard Cincotta
..... Judith S. Siegel
..... David Hamill

USIA's electronic journals, published and transmitted worldwide at three-week intervals, examine major issues facing the United States and the international community, and inform foreign publics about the United States. The journals — ECONOMIC PERSPECTIVES, GLOBAL ISSUES, ISSUES OF DEMOCRACY, U.S. FOREIGN POLICY AGENDA and U.S. SOCIETY AND VALUES — provide analysis, commentary, and background information in their thematic areas. All journals are translated into French and Spanish, with the Hypertext versions published one week after the English; the Adobe Acrobat versions appear shortly thereafter. Selected issues are also translated into Arabic, Chinese, Portuguese, and Russian, with the latter two appearing on Hypertext and Adobe Acrobat versions. The opinions expressed in the journals do not necessarily reflect the views or policies of the U.S. Government. Articles may be reproduced and translated outside the United States unless there are specific copyright restrictions cited on the articles. Current or back issues of the journals can be found on the U.S. Information Service (USIS) Home Page on the World Wide Web at "<http://www.usia.gov/journals/journals.htm>". They are available in several electronic formats to facilitate viewing on-line, transferring, downloading, and printing. Comments are welcome at your local USIS office or at the editorial offices: Editor, Global Issues (ITGIC), U.S. Information Agency, 301 4th Street SW, Washington, D.C. 20547, United States of America. You may also communicate via email to ejglobal@USIA.gov.

FOCUS



A MARKET FOR JUST ABOUT ANYTHING

Vice President Al Gore

Excerpted from the vice president's remarks July 1 at the release of the White House report on the "Framework for Global Electronic Commerce."

One of the Internet's most lasting impacts may be just beginning to unfold. The information superhighway promises to utterly transform commercial transactions. How we buy and sell the stuff of our lives.

More than a century ago, if you wanted to raise money for a business — even a large one — you practically had to go door-to-door looking for someone to buy a stake. But Wall Street and the stock exchange changed that. They established a market for capital, linking people who wanted to purchase company shares with people who wanted to sell them.

In much the same fashion, the Internet can create a market, a global market, for just about everything else.

Already you can use the Internet to send flowers to your spouse, or order a book, or make travel reservations and buy a ticket. And that's just the very beginning. Pretty soon you'll be able to buy just about anything on line. You'll be able to find the best price in the world almost instantly from

your home computer. And you'll be able to do it in a virtual shopping mall that is open all day, all night, every day, all across the world.

In this emerging digital marketplace, nearly anyone with a good idea and a little software can set up shop and become the corner store for the entire planet. That promises to unleash a revolution in entrepreneurship and innovation, a cascade of new products and services that today we can scarcely imagine.

With the framework (for electronic commerce) we are helping to make sure that commerce goes digital, that business goes global, and that ingenuity goes wild.

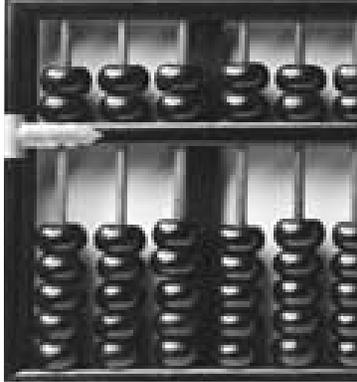
In essence, we're defining government's role in these early days of the Internet. We're saying that our (governmental) approach to electronic commerce must be guided by a digital Hippocratic oath: "Do no harm."

The Internet moves too quickly for heavy-handed government regulations. Were we to apply such rules to this emerging marketplace, the rules would likely be obsolete before they hit the law books, an impediment to individual creativity rather than a safeguard of the common good.

If we move to heavily regulate something whose form changes so quickly and so often, we risk suffocating the very essence of the Internet.

In order to realize its full promise, we must give the Internet room to breathe and continue growing. But equally important, we must make sure the Internet has room for everyone.

A proper framework for promoting private commerce requires an unwavering commitment to protecting the public interest, and here government does have a role, working with the private sector to preserve individual privacy, to protect intellectual property, to promote fair competition, and to ensure open access.



COOPERATION NEEDED

William Daley
Secretary of Commerce

Excerpts of remarks made July 8, 1997, at the European Ministerial Conference on Global Information Networks held in Bonn.

As we consider how the day-to-day affairs of business — negotiating, comparing, contracting, selling, bidding, bargaining, buying — are to be done via the Internet and the Global Information Infrastructure, we have one option: to move forward as partners. To do less is to risk turning this next great economic stage into another dividing line among nations, where language, culture, geography, currency, history, and technology still keep us from working together.

We are in a very fortunate position. The technology needed for electronic commerce already exists and is in place, right now connecting some 60 million people around the world in a seamless network.

Any transaction that is done from a distance, be it by telephone, fax, or mail, can be done cheaper, faster, and easier on the Internet. And given that in less than 15 years an estimated 1,000 million people around the world, nearly 20 percent of the global population, will be linked by the Internet, it is almost inescapable that the most efficient way to reach the most consumers in the global

economy will be via electronic commerce. With the technology and the infrastructure in hand, the challenge before us is to deliver on this promise.

Again, we are in a very fortunate position. Because the principles most important to the Clinton administration for the Internet marketplace are shared by our allies in Europe.

We agree that electronic commerce will rely upon private sector-led solutions and market-driven possibilities. It will not be, and should not be, a government run marketplace. In fact, the government's role should be minimal: over-regulation should be avoided; those rules now on the books that are out-of-date or hinder electronic commerce should be revised or eliminated; and contractual agreements where buyers and sellers come together freely should rule the day.

When regulations are a must, they should be technology neutral, because emerging technology will outstrip regulations as fast as they are put in place, and should simply foster competition, protect intellectual property and privacy, and prevent fraud.

The pace of change in technology and in the applications of electronic commerce demand a

new way of solving problems, driven by leaders in business and industry. One instructive example: Microsoft and Netscape put their combined talents and resources together to make sure using the Internet doesn't invite privacy abuses such as creating unintended access to files or networks.

This is how electronic commerce must evolve and be managed — because it is business that has most vested in the success of electronic commerce, and that can only happen if business gives consumers around the world the confidence and the trust to transact on the Internet.

With the shared goal of a thriving, growing, and prosperous marketplace on the Internet, the issue is how to get there. President Clinton in July 1997 unveiled nine recommendations to guide American efforts with our partners to spur electronic commerce, and to ensure it evolves in the most useful, efficient way for all participants. They are:

- The Internet should be declared a free trade zone — a tariff-free environment whenever it is used to deliver products or services.

- Because electronic payment systems are still emerging, it would be hard to develop a policy that is both timely and effective. Inflexible rules and regulations for electronic payments should be avoided in favor of case-by-case monitoring as payment systems evolve.

- Parties should be able to do business with each other on the Internet under whatever terms they agree upon. But predictable and widely accepted legal principles to support electronic commerce are essential for private enterprise and free markets. We will work for an international uniform commercial code to simplify and encourage electronic commerce under consistent rules and rights.

- We must protect intellectual property rights, so that music, movies, and art are available but that the piracy that already robs them of nearly \$11,000 million in earnings does not explode in a global electronic marketplace. Sellers must know their intellectual property will not be stolen, and buyers must know they are getting authentic products. International agreements that establish clear copyright and patent and trademark

protection to protect against piracy and fraud are a must.

- It is essential to ensure privacy in the networked environment if people are to feel comfortable doing business in this electronic marketplace. We must work to protect children while respecting the rights of business. And we must protect the privacy rights of consumers, so that privileged information that is useful for one transaction does not place them at the mercy of others.

- We must guarantee security by allowing sophisticated encryption to protect data like credit card numbers or detailed contracts from being read during transactions; but we must also make sure national security is safeguarded by applying those rules sensibly, so that potential terrorists or other sophisticated criminals cannot hide their work behind encryption technology.

- We must work with partners around the world to insure uniform rules and uniform rights, otherwise electronic commerce threatens to become little more than high tech isolationism; and we must work together to build a modern global telecommunications network that is accessible, affordable, and supports electronic commerce.

- The Internet carries more information and content than traditional TV or radio ever could, but also offers users greater opportunities to control content and access. Regulations that are now routinely applied to objectionable content in broadcasts do not, and should not, apply to the Internet. Instead, industry self-regulation, technical solutions like filters and age verification, and rating systems should be adopted internationally to protect people from objectionable material rather than content quotas or burdensome regulations.

- And the marketplace should determine technical standards — technology is moving more rapidly than lawmakers can respond, and attempts by government to manage the Internet will only inhibit technological innovation.

We know that on some details of electronic commerce we have different ideas. Discussions on

non-tariff barriers to content, balancing encryption for privacy needs with national security concerns, varied technical standards, and digital signatures should be on-going.

The United States has very definite positions and we have every reason to be confident that we will bridge the gap between us. Still, given the wide and diverse areas to be covered in building this electronic marketplace, the fact is there is much more common ground than disparity between the Bonn conference declaration and the United States' recommendations.

Electronic commerce should be the ultimate business and information vehicle — a growth economy that can fuel small start-up companies, help businesses grow, and give corporations access to new, promising markets while also offering education and communication resources. All with little bureaucratic interference.

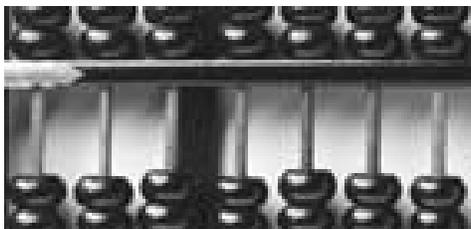
How it evolves, the contributions it makes to creating jobs, improving standards of living,

helping consumers, spurring economic growth, and bridging gaps between people will be best led by our private sectors and with our cooperative efforts.

We must avoid having this new electronic world become a digital divide — electronic commerce must respect every society, be accessible to every community, and deliver benefits to all who participate.

Concepts like open markets, free trade, privacy, and rule of law are the very foundation upon which electronic commerce must be built.

When President Clinton announced his administration's electronic commerce initiative, he explained, "Our task is to make sure electronic commerce is safe and stable terrain for those who wish to trade on it. And we must do so by working with other nations now, while electronic commerce is still in its infancy."



GLOBAL PARTNERSHIP FOR E-COMMERCE

An interview with Ira Magaziner, senior advisor to the president for policy development.

Magaziner was director of the study that produced the White House report, "A Framework for Global Electronic Commerce." He says that a global partnership is needed to build a digital economy. Magaziner was interviewed by Edmund F. Scherr.

Question: What is the purpose of the electronic commerce report?

Magaziner: The emerging digital economy has the potential to be an engine of growth for the world economy for the next quarter of a century if we can put the right framework in place to allow it to grow and flourish. The purpose of this report is to try to initiate a series of global discussions in order to create a framework that will allow electronic commerce and the new digital economy to emerge in as healthy a way as possible.

Q: Please describe the international effort to encourage electronic commerce.

Magaziner: The U.S. government is trying to work as equal partners with other governments and with the world's business community to try to help create the architecture for this future digital

economy.

We believe this should be a cooperative effort. We don't believe that any of us has all the right answers. None of us knows for sure how this marketplace is developed, and how the technology is going to develop. So, we need to work together to create the sort of commercial and legal and economic frameworks that will allow this new economy to emerge.

We don't view the international discussions that we are now embarking upon as traditional trade negotiations where we knock heads with the countries and try to change each other's systems. What we want to do is to create a common framework for what will be the first real industry that's born globally.

Q: What has been the international response to the report?

Magaziner: In the United States we've had a tremendous outpouring of support from industry, Internet users, and the general public. Abroad, in my meetings to discuss the president's initiative, we have been very encouraged by the fact that in many countries electronic commerce is now a front-burner issue. It's being viewed as very

significant in those countries, and there seems to be, in general, a support for the kind of principles that we are promoting.

While there are many issues that need to be worked out in detail as we go through a discussion process, we have been very encouraged so far with the reception.

Q: Can you pinpoint any actions by other countries that have been energized by the framework report?

Magaziner: For the most part, the issue is still at the discussion and policy level. But, for example, the Japanese Ministry of International Trade and Industry has issued a report. The European Union has also issued a report on electronic commerce.

We know that a number of governments have also now initiated processes to develop their own policies or to accelerate development of policies.

Q: Can you describe the growth of electronic commerce?

Magaziner: The electronic marketplaces really just began to take off about a year ago. There are forecasts, which we think are realistic, that while electronic commerce represents only about \$2 billion (\$2,000 million) of company buying on the Internet today, by the year 2002 it will represent almost \$300 billion (\$300,000 million) of business just in the United States.

We also can see a tremendous amount of activity as companies begin to set up their customer-service functions on the Internet. We're beginning to see now the development of retail activities on the Internet — the selling of books, flowers, automobiles, and a whole range of other products and services. Also, we see the development of new businesses that are digitally delivering services, like downloading audio recordings or news services. The whole arena of electronic commerce is only one or two years old, but we think the growth will be exponential.

Q: Are there some areas of electronic commerce growing faster than others?

Magaziner: It's hard to say what will develop the fastest. Certainly the financial-service industry is moving very rapidly to deliver its services across the Internet, and business-to-business applications — businesses doing purchasing or customer relations — are growing very rapidly. The airline and travel industries are doing an increasing amount of selling across the Internet. There are businesses on the Internet that are aimed at special interest groups — whether new parents or flower growers, for example.

Q: Is there a need for international agreements to foster electronic commerce?

Magaziner: Since the Internet is being born globally as a marketplace, we are hoping to get international agreements on a market-proven approach to the Internet so that there would be a minimum of regulation globally. There needs to be tax agreements negotiated so that there is uniformity, and we're hoping to get government agreements to make the Internet a zone that's free of customs duties — a tariff-free zone. So, there is a variety of areas where we hope to get government agreements to allow the market to develop.

Q: How will electronic commerce encourage a free and open global marketplace?

Magaziner: The Internet will be a global medium. By the year 2005, there will be over a billion people on the Internet, and we do not want artificial barriers put up to prevent those people doing business with each other.

We're hoping to get agreements to eliminate nontariff-trade barriers. There are cases where telecommunications requirements hinder the flow of information. We would like the flow of information to be free of censorship, and we'd like to have agreement that there not be tariffs, no undue taxation for electronic commerce.

Also, we are hoping that there can be some affirmative steps put in place where governments do need to act. For example, that we develop a uniform commercial code globally so that a digital signature or a contract made electronically is valid across national borders or that intellectual property

be protected across international borders. So there is a need for some affirmative agreements as well as some agreements for governments not to interfere.

Q: How will the Internet affect developing countries?

Magaziner: We think that the Internet will have one of two possible effects, and it's very important that we bring about the right one of these two.

If the Internet is only available in developed countries, then we could have a very bad development where essentially the Internet was a force that increased the disparity of incomes in the world. However, if the Internet comes to developing countries, then we think it will be a force for narrowing the income gap in the world. The Internet can be a very positive force for economic and social development.

The beauty of the Internet is that because satellite and wireless technology will be in place early in the next century, it will be cheaper to bring the Internet to poor and rural countries than to bring the telephone right now. It is a technology which can make it easier for educational materials, health-care diagnostic materials, news, and other information areas to permeate developing countries.

The Internet can make it easier for companies in developing countries to do business globally. It is now very difficult for a small company in a developing country to be part of the global marketplace. But with the Internet, you can set up and immediately have access to a billion people globally as a market. If the Internet can reach the developing world, it can be a great force for economic and social development.

That's the reason we're supporting efforts by various development banks to sponsor Internet-related projects. If local area networks can be built up in developing countries, then they can hook up to the Internet through satellite, and that will accelerate the growth process.

The Internet is now in some 150 countries, and so it is beginning to permeate into developing nations. The key is for the Internet to spread out

within those countries so it's accessible not just in the capital city, but also throughout the country, and that's where we think the satellite wireless technology can help.

Q: What are the roles of the private sector and governments in developing electronic commerce?

Magaziner: Overall, we think the private sector needs to lead the development of the new digital economy and that the digital age moves too quickly and is too unpredictable for governments to play a heavy role. Even where collective action is necessary, we think that private collective action is preferable to government-directed action or government regulation.

Now, there are some exceptions to that. Obviously, governments are involved with taxation. Governments need to be involved in protecting intellectual property. Governments need to be involved in helping set a uniform commercial code so that there can be a unified, legal basis to conduct contracts and other such things, but the government role should be focused and transparent and targeted.

Q: What is the administration's position on the export and use of encryption technology?

Magaziner: We're trying to strike a balanced approach between two concerns. From a purely commercial point of view, you want high-level encryption that can be used so that transmissions can be private and secure, and which will ease the conduct of commerce. From a law enforcement point of view, there is a concern that high-level encryption could be used by terrorists and drug dealers and other criminals to do their business and hamper law enforcement.

So we've been trying to strike a balanced approach that allows high levels of encryption to be used in commerce, but which also allows law enforcement to have the potential for access in cases where there is clear justification under our legal system that a criminal act may be committed.

Edmund F. Scherr writes on information technology and other global issues for the United States Information Agency.

COMMENTARY



NEW PRODUCTS, SERVICES NEEDED

An interview with Vinton Cerf, senior vice president for Internet Architecture and Engineering, MCI Communications Corporation

Cerf, recognized as one of the pioneer developers of the Internet, says that in electronic commerce the real challenge is to develop new products and services for this new form of business.

Question: How will industry leaders convince those skeptical of technology that electronic commerce is not a passing fancy, and that it can be easier than a telephone toll-free number or direct mail marketing?

Cerf: Part of the answer is making transactions secure. That, of course, is only half the battle. The real challenge will take place when and if business develops products and services that are more than just digitized versions of traditional business. Look at the automobile industry initiative which is aimed at automating business transactions between the automobile manufacturers and their thousands of suppliers.

Right now, the best example of success in electronic commerce is Amazon.com, the online bookstore. But, eventually, we're going to need to

see the development of applications that are unique to the Web, otherwise, electronic commerce will just be an engine for replacement, not new economic growth.

Q: What are the privacy issues in electronic commerce? What are the possible solutions?

Cerf: There is universal agreement that privacy needs to be protected on the Internet, but agreement frays when deciding exactly how this is to be done.

The current U.S. law protecting individual privacy is basically sound, but there are many voices on this subject and not all of them agree. In other parts of the world, privacy concerns have led to legislated and potentially bureaucratic methods that do not comport well with the fast-moving, highly connected Internet environment.

Industry is working with with the Internet Privacy Working Group and the World Wide Web Consortium to develop standards and software to allow consumers to assert their preferences in the use of personal information.

Individuals should be able to control what personal information can be obtained on the Net and should be informed as to the use that businesses intend to make of any personal information obtained in the course of normal Internet interaction.

Q: How should the problem of encryption be handled to tackle both commercial and security needs? Is there a compromise? How important is this issue to the development of electronic commerce?

Cerf: It is no surprise that, in today's wired world, cryptography is most often being applied to the fledgling field of electronic commerce.

Despite the small chances of interception of confidential financial information, such as a credit card number, many individuals still do not trust shopping on the Internet. Mostly this is owed to the relative youth of the process, but this does not relieve us of the responsibility to develop structures that authenticate both the identity of seller and purchaser, and insure the confidentiality of the transaction contents.

It seems likely that the fastest growth area will be business-to-business commerce. What many businesses are discovering is that potential efficiencies will not be realized without also including the potential for transactions between companies. The relative sizes of the transactions dictate a strong need for source validation and integrity protection to resist hacking.

Q: How about the issue of Internet domain names? How will this impact on development of electronic commerce?

Cerf: The current controversy on domain names (the registration and use of domain names — the names of companies, products, government bureaus, etc., used in Internet addresses) is only tangentially involved in the development of electronic commerce — mostly in terms of trademark law. It really has more to do with ensuring the continued growth of the Internet, primarily by introducing competition to the business of assigning domain names.

In the long run, alternative ways of drawing attention to corporate products without overuse of domain names for trademarked product names may well relieve some of the pressure. Other intellectual property issues also deserve attention, particularly copyrights in an online, digitized world.

Q: Will PCs or network computers be the best access point for electronic commerce in the future?

Cerf: I think either platform could serve just as well as a public access point for electronic commerce. In general, I believe anything that helps speed the delivery of the power of the Internet into as many hands as possible is good for society, and for business as well. When we talk about network computers, we should be careful to also consider Internet appliances like add-on connections through TV set-top box products.

The key here is making inexpensive access to the Internet available as widely as possible. In this case, I think network computers could, in theory, speed the growth of electronic commerce by increasing the pool of potential customers. However, it seems clear to me that both platforms will co-exist in the future.

Q: What will happen to the virtual shopping malls on the Web that were all the rage in 1995-96, but are petering out? Will they evolve into other forms? How will the telecom carriers work to reduce prices to make it easier to use a PC than a telephone and mail catalog for the home shopper?

Cerf: I think the re-introduction of the virtual shopping mall is just around the corner. The next logical step for electronic commerce is in intra-business applications, involving corporate intranets and immense vertical industries like auto manufacturing — say Chrysler ordering hundreds of thousands of windshields a month from Pittsburgh Plate Glass.

In terms of the virtual shopping mall, those who captained the initial foray into electronic commerce didn't fully take into account how excessive download times made shopping by Internet a trying experience at times.

Shopping, for many, is still an experience for the senses. And, even being able to duplicate the efficiencies of a glossy mail-order catalog online was nearly impossible when you're relying on a 33.6 kbps (kilobytes per second) modem. Once we solve the problem of delivering broadband access to the home, most likely through the widespread deployment of cable modems in the U.S. and other technologies in Europe, we will see the resurrection of the virtual shopping mall.

In the meantime, products that require configuration and the like will thrive because Web-enabled searching and selection and configuration will assist buyers and relieve customer service loads.

Q: Which countries will be the vanguards in promotion of electronic commerce?

Cerf: By virtue of its head start in the development of Internet infrastructure, it is safe to believe the United States will be first in participating in electronic commerce.

But, the development of e-commerce is more than just a question of infrastructure, it also is closely tied to the development of Internet-friendly

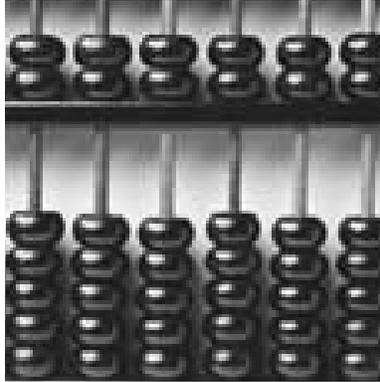
policies. All sorts of legal and regulatory roadblocks stand in the way of the development of unfettered and secure Internet commerce.

From copyright and intellectual property laws to the threats posed by the over 30,000 taxing authorities in the United States who could claim some jurisdiction over Internet transactions, to the development of standards for digital signature that could aid authentication, there are still many issues to be resolved.

At this point, it would be good to recognize the Clinton administration for its work in encouraging legal frameworks friendly to the development of electronic commerce.

Cerf is the co-creator of the TCP/IP computer networking protocols that became the language for Internet communications. An expert in Internet development and technologies, Cerf was the founding president of the Internet Society. Cerf's Web page can be accessed at: <http://www.mci.com/aboutyou/interests/technology/ontech/cerf.shtml>

In keeping with the information age, the journal's editors interviewed Cerf through an exchange of e-mail messages.



THE INTERNET HAS COME OF AGE

Louis V. Gerstner, Jr.
Chairman and Chief Executive Officer
IBM Corporation

Excerpts from remarks made July 1, 1997, at an event marking the release of the White House report, "The Framework for Global Electronic Commerce."

Today, 50 million people are connected to the Internet. That number will probably grow to 500 million, and some even predict a billion people will one day use the Net.

The number-one question that I get from people as I go around the world, particularly if they're over 40, is: What are all these people going to do when they're connected to the Net? The answer is, all the things they do today. They will buy and sell; bank; get entertainment; trade stocks; earn a college degree; replace a driver's license.

This is what we mean by e-commerce. It's not just about buying and selling over the Net. It's about using this powerful new technology to transform every aspect of what we do as people.

A lot of important pieces had to be put in place before e-commerce could take hold: new technologies; agreements on standards for things like secure financial transactions; and, significantly, leadership initiatives like the policy framework for electronic commerce.

But these elements are now in place. Today we can say with confidence: The Internet is not only open for business, it's ready for business. The Internet has come of age.

For enterprises, it represents enormous opportunity, because networks are great levelers. They dissolve many traditional barriers to entry.

We all know that "location, location, location" is a tenet of good business. Increasingly, the Net is where business must be. With a first-class web site, any business of any size can challenge entrenched franchises and brands, anywhere in the world.

The potential is huge for businesses that move to the Net quickly. Some estimate that e-commerce volumes today are about \$2 billion — and will grow to more than \$1 trillion (\$1,000,000 million) by the year 2010.

Millions of people who are connected to the Net and who are asking, "What do I do with it?" They can now dive into the richest, most diverse, borderless, sleepless marketplace the world has ever seen.

And, as they shift from “browsing” to buying, they can do so with greater confidence that their transactions will be secure and their private information will remain private.

As exciting as all of this is, commerce is only one type of human activity this technology is transforming.

As with the electric light, the printing press, and manned flight — other great technologies the world has seen — information technology is transforming and will continue to transform everything. It will vastly improve every aspect of society and human interaction: how we’ll make the arts available to all; how we’ll receive government services; how we’ll care for our elderly and homebound.

With networks we have the chance to deliver the best, to the neediest: the best teachers to our most remote rural school districts or the forgotten enclaves of our inner cities; the skill of the finest physicians to patients in need, without regard for physical proximity; and knowledge about the

world to all the people in the world.

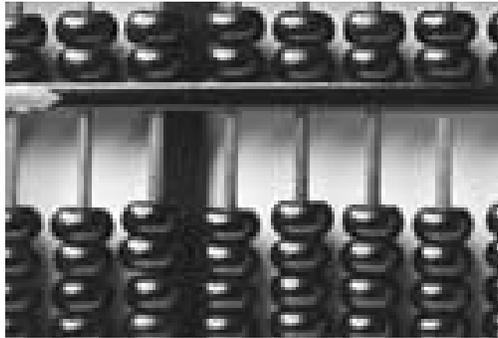
Of course, as all of this takes off, it spawns a range of societal and technology issues. Some we recognize as old issues in new garb, along with new challenges dealing with taxation, security, and parental responsibility.

The answers to those issues begin with the kind of leadership that has resulted in the policy framework: government and industry working together, defining appropriate roles and responsibilities.

This sends a very powerful message: The private sector, an open marketplace, and competition — not the government — will regulate opportunity and the pace of innovation.

Industry welcomes these initiatives.

And we are committed to work with the administration, with Congress, and other governments to make the recommendations in this report a reality and to fully deliver the promise of a networked world.



KEEP BIG BROTHER'S HANDS OFF THE INTERNET

By Senator John Ashcroft,
Republican, Missouri

Chairman of the Senate Commerce Subcommittee on Consumer
Affairs, Foreign Commerce and Tourism

The Internet provides a great opportunity to our country, in part by representing the most inviting form of communication ever developed. It draws people together from all corners of the globe to share and communicate on an unprecedented level, and brings all branches of government closer to the public that they serve.

The Internet allows small businesses to reach out across the globe and conquer the distances between them and potential customers. Individuals can view merchandise and make purchases without leaving home. The Internet also holds great promise for education. Students — rural, suburban, and urban — are increasingly able to access a wealth of information with their fingertips that was previously beyond their reach.

In order to guarantee that the United States meets the challenge of this new means of commerce, communication, and education, government must be careful not to interfere. We should not harness the Internet with a confusing array of intrusive regulations and controls. Yet, the Clinton administration is trying to do just that.

The Clinton administration would like the Federal government to have the capability to read any

international or domestic computer communications. The FBI wants access to decode, digest, and discuss financial transactions, personal e-mail, and proprietary information sent abroad — all in the name of national security. To accomplish this, President Clinton would like government agencies to have the keys for decoding all exported U.S. software and Internet communications.

This proposed policy raises obvious concerns about Americans' privacy, in addition to tampering with the competitive advantage that our U.S. software companies currently enjoy in the field of encryption technology. Not only would Big Brother be looming over the shoulders of international cyber-surfers, but the administration threatens to render our state-of-the-art computer software engineers obsolete and unemployed.

There is a concern that the Internet could be used to commit crimes and that advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?

The protections of the Fourth Amendment are clear. The right to protection from unlawful searches is an indivisible American value. Two hundred years of court decisions have stood in defense of this fundamental right. The state's interest in effective crime-fighting should never vitiate the citizens' Bill of Rights.

The president has proposed that American software companies supply the government with decryption keys to high level encryption programs. Yet, European software producers are free to produce computer encryption codes of all levels of security without providing keys to any government authority. Purchasers of encryption software value security above all else. These buyers will ultimately choose airtight encryption programs that will not be American-made programs to which the U.S. government maintains keys.

In spite of this truism, the president is attempting to foist his rigid policy on the exceptionally fluid and fast-paced computer industry. Furthermore, recent developments in decryption technology bring into question the dynamic of government meddling in this industry. Three months ago, the 56-bit algorithm government standard encryption code that protects most U.S. electronic financial transactions from ATM cards to wire transfers was broken by a low-powered 90 MHZ Pentium processor.

In 1977, when this code was first approved by the U.S. government as a standard, it was deemed unbreakable. And for good reason. There are 72 quadrillion (72,000 trillion) different combinations in a 56-bit code. However, with today's technology these 72 quadrillion combinations can each be tried in a matter of time.

Two days after this encryption code was broken, a majority of the U.S. Senate Commerce Committee voted, in accordance with administration policy, to force American software companies to perpetuate this already compromised 56-bit encryption system. In spite of the fact that 128-bit encryption software from European firms is available on Web sites accessible to every Internet user. Interestingly, European firms can import this super-secure encryption technology (originally developed by Americans) to the United States, but U.S.

companies are forbidden by law from exporting these same programs to other countries.

I believe that moving forward with the president's policy or the Commerce Committee's bill would be an act of folly, creating a cadre of government "peeping toms" and causing severe damage to our vibrant software industries. Government would be caught in a perpetual game of catch-up with whiz-kid code-breakers and industry advances. Senate Majority Leader Trent Lott has signaled his objection to both proposals.

The leader and I would like to work to bring solid encryption legislation to the Senate floor. Any proposal should give U.S. encryption software manufacturers the freedom to compete on equal footing in the international marketplace, by providing the industry with a quasi-governmental board that would decide encryption bit strength based on the level of international technological development.

U.S. companies are on the front line of on-line technologies — value-added industries of the future. Consider this: Every eighteen months, the processing capability of a computer doubles. The speed with which today's fastest computers calculate will be slug-like before the next millennium or the next presidential election comes along. The best policy for encryption technology is one that can rapidly react to breakthroughs in decoding capability and roll back encryption limits as needed.

The administration's interest in all e-mail is a wholly unhealthy precedent, especially given this administration's track record on FBI files and IRS snooping. Every medium by which people communicate can be subject to exploitation by those with illegal intentions. Nevertheless, this is no reason to hand Big Brother the keys to unlock our e-mail diaries, open our ATM records, read our medical records, or translate our international communications.

Additionally, the full potential of the Internet will never be realized without a system that fairly protects the interests of those who use the Internet for their businesses, own copyrighted material, deliver that material via the Internet, or individual

users. The implications here are far-reaching, with impacts that touch individual users, companies, libraries, universities, teachers, and students.

In December 1996, two treaties were adopted by the diplomatic conference of the World Intellectual Property Organization (WIPO) to update international copyright law. These treaties would extend international copyright law into the digital environment, including the Internet. However, these treaties do not provide a comprehensive response to the many copyright issues raised by the flourishing of the Internet and the promise of digital technology. We must work to keep the scales of copyright law balanced, providing important protections to creators of content, while ensuring their widespread distribution. In an attempt to meet these goals, I introduced the Digital Copyright Clarification and Technology Education Act of 1997.

Equally important, we must begin a process that is structured to balance the rights of copyright owners with the needs and technological limitations of those who enable the distribution of the electronic information, and with the rights and needs of individual end users. The current treaties and statements are not sufficient, and include some language that could create legal uncertainty. This vague language could lead to laws that ignore technical realities. The language must be clarified through the enactment of legislation in conjunction with the Senate's ratification of the treaties.

Another issue that could prevent the Internet from reaching its potential is taxation. If we tax the Internet prematurely or allow discriminatory taxing, we may stifle a burgeoning technological development that holds much commercial, social, and educational promise for all Americans. Taxation should be considered only after we have fully examined and understood the impact that unequivocal taxation would have on this new means of commerce. The Internet Tax Freedom Act would allow for full consideration of the opportunities and possible abuses by placing a moratorium on further taxation of online commerce and technologically discriminatory taxes. It is important to note that S. 442 will allow states and local jurisdictions to continue to collect any tax already levied on electronic commerce.

On-line communications technology is akin to the Wild West of the 19th century. To best settle this new frontier, we should unleash American know-how and ingenuity. The government's police-state policy on encryption is creating hindrances and hurdles that will eventually injure our ability to compete internationally. Government's role should be to break down barriers, to allow everyone to excel to their highest and best.

Senator Ashcroft is a member of the Senate Commerce, Judiciary, and Foreign Relations Committees. His Web homepage is: <http://www.senate.gov/~ashcroft/> and his e-mail address is: john_ashcroft@ashcroft.senate.gov



THE RISKS AND REWARDS

By Larry Irving

Assistant Secretary of Commerce for Communications and Information

The "Economist" magazine notes that technological turning points are difficult to spot. The publication pointed out that at the turn of the century when Studebaker switched from making horse-drawn carriages to making cars, the move was not obvious because in the previous five years New Yorkers had bought 350,000 carriages and only 125 cars.

Now we are entering a new century, and the information age is about change and about achieving new impossibilities. This change will affect businesses. They need to understand it and, more importantly, take advantage of it.

Businesses of all sizes need to understand the role that telephones, computers, networks, and technology can play in creating new impossibilities. And if they can harness this potential, they will be the successful entrepreneurs and business persons who will bring new products to the market, increase consumers' choices, lower costs, and improve national economies.

Just consider for a moment the changes that have taken place in the telecom and information sectors in the last several decades. The global network of computers, telephones, and televisions has

increased its information-carrying capacity a million times over. In 1960, a transatlantic telephone cable could carry only 138 conversations simultaneously. Today, a fiber-optic cable can carry 1.5 million conversations at one time. Today's laptop computers weigh as little as 1.85 pounds (0.83 kilograms) and are many times more powerful than the \$10 million mainframe computers of the mid-1970s. Twenty-five years ago there were only about 50,000 computers worldwide; today that number is estimated at 140 million. And no communications medium has ever grown as fast as the Internet, which has an estimated 50 million users worldwide.

Two key issues are emerging as increasing numbers of individuals and companies use electronic networks to engage in commerce: (1) the need for companies to focus on their value-added; and (2) the need to delineate the appropriate roles of the private sector and the government.

The Risks and Rewards for Businesses —

The explosive pace and unpredictable nature of the technological developments make any attempt to engage in electronic commerce a bit like betting on a long-shot in a horse race. Even industry leaders don't always make it to the winner's circle.

The Internet, Intranets, extranets, and other communications networks are lowering entry barriers to commerce, enabling both small and large firms as well as consumers to engage in and benefit from electronic commerce. Electronic commerce is already generating important sales and savings for businesses.

For example, the on-line bookseller Amazon.com's increasing share of the bookstore market (by offering discounts up to 40 percent) forced major bookstore chains like Barnes & Noble and Borders Books to go on-line. Federal Express delivery service saved as much as \$10,000 a day in 1996 by moving some of its customer service to its Web site. Dell Computer now sells \$1 million worth of PCs every day on the Web. General Electric buys \$1,000 million in materials from suppliers on-line and saves money by streamlining the process and opening it up to more competition.

Keep in mind that it is not simply a matter of creating a Web site. Amazon.com is a success, now valued at \$500 million. Interestingly, a British businessman pursued the same idea at the same time — but his company is only worth \$3 million today. Why the difference? Jeff Bezos, the American owner of Amazon.com, researched the industry and relocated to be near one of the world's biggest book warehouses. Mr. Bezos also raised \$11 million from venture capitalists at the outset and heavily marketed his business. And he learned how to market effectively worldwide — Amazon.com sales outside the United States are 10 times the British company's sales outside of Britain.

Electronic commerce is not just for big corporations. In fact, it provides exciting possibilities for small companies and entrepreneurs to tap into markets around the world. Moreover, it enables the sharing of valuable information and resources. Recently, Women Inc. (a non-profit organization devoted to helping women business owners succeed) and AT&T announced a partnership that will greatly help women entrepreneurs and could serve as a model for other groups. AT&T has provided Women Inc. with a \$25,000 grant to develop and host a Web site that will give Women Inc. members data space for business transactions, space to sell their products and services, the opportunity to "ask the expert"

business-related questions, and the ability to register for conferences. Through the Web site, members also have access to a host of services.

The Internet is causing a lot of businesses to rethink how they do business. Business owners and executives should ask themselves: "If the Internet, in its current state, had been around when the enterprise was founded, would you be running your business the way you are doing so today?" If the answer is no, why not change now? Can you develop a niche market? How can you compete effectively with off-line companies as well as other on-line companies?

Private Sector, Government Roles —

The Clinton administration believes that the private sector can and should develop many of the solutions to emerging legal, policy, and technical challenges with respect to electronic commerce, particularly activities on the Internet. When activities on the Internet raise new issues, the government should first turn to the private sector to see if a solution can be crafted without government action.

The Internet community has a demonstrated record of expanding the Internet, successfully managing its operation and growth, and developing policies and mechanisms to govern its use without government regulation.

Many of the solutions to emerging Internet-related concerns lie with technology, and in turning to the private sector we can take advantage of its entrepreneurial energy. The private sector has already demonstrated its ability to develop new technology tools, such as screening software to address concerns about children's access to adult material on the Net, as well as standards that would give individuals the ability to control the disclosure and use of their own personal profiles generated when using the Web.

The U.S. federal government does have a valuable, and at times critical, role to play with respect to the development of electronic commerce. The federal government should be engaged in: (1) promoting a market-driven environment; (2) creating a predictable legal environment governing electronic commerce transactions, and (3) building

business and consumer awareness about externalities that undermine healthy markets.

Even as the government takes steps to fulfill this role, we must ensure that any government action is the minimal necessary to achieve goals and one that allows competition and innovation to flourish.

A Market-Driven Environment —

The federal government has a valuable role to play now to preserve the global environment in which a contract-based, market-driven model of commerce can emerge. Increased commercial activity on the Internet makes it an increasingly attractive target for government regulation to address concerns about fraud, content, and competition, as seen by recent state and foreign government action. Consequently, the federal government has two distinct, but complementary, roles:

(1) U.S. leadership is needed to preserve the Internet as an unregulated, contract-based, market-driven environment internationally as well as interstate.

(2) In some cases concerted international, intergovernmental action will be needed to facilitate electronic commerce and protect consumers. In these cases, U.S. leadership is needed to promote a minimalist approach designed to ensure competition, prevent fraud, foster transparency, and facilitate dispute resolution.

The Clinton administration believes that government should minimize regulations and let technology blossom and grow. The administration's approach to the Internet is that, in general, our first instinct should be to refrain from regulation. No form of electronic media has grown as fast as the Internet, and the Net has grown precisely because it is not regulated.

We are very concerned that a number of nations have taken steps or are contemplating action to censor information received by their citizens via the Internet. We believe that freedom of speech applies in cyberspace and that laws censoring the information that flows over the Internet are both misguided and impractical, especially given the global nature of the Internet.

We strongly believe that the best way to fight misinformation is with more information. To quote actress Mae West: "Too much of a good thing is wonderful." Moreover, the best guarantee of democracy and stability are informed citizens.

Obviously, on certain issues such as pornography and children's access to adult material, the U.S. government is concerned. But even here, we are looking to industry to self-regulate and to develop technological tools that parents and Internet service providers, not the government, can use to filter out material inappropriate for children.

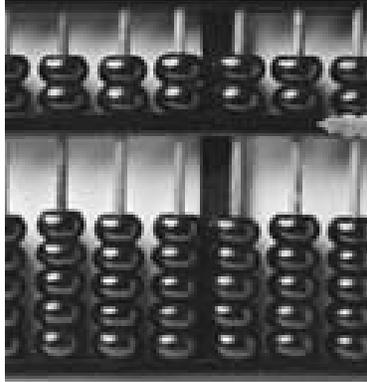
The good news is that the computer industry and the on-line service industry have been moving quickly and responsibly to develop new products and services to make the Internet "family-friendly." These technologies enable parents — not governments — to determine what is appropriate for their children.

The Internet and its products also are generating new competition for traditional telecommunications and media companies. The Clinton administration is concerned with recent attempts by other nations to ban or block telephone calls on the Internet to protect their state-owned phone companies.

A Predictable Legal Environment —

The U.S. government has an important role to play as facilitator and catalyst for electronic commerce. We need to examine whether existing governing standards should continue to apply and whether new ones are needed. The major issues include data security, intellectual property, privacy, and financial issues.

The United States recognizes that other nations are facing these same issues, yet often with a different historical and cultural perspective as well as different legal and regulatory frameworks. Given the global nature of the Internet and other networks, a consensus regarding governing standards needs to be developed on both national and international levels.



SECURITIES FRAUD LOOMS AS DARK SIDE OF INTERNET GROWTH

By Jim Fuller

A business partnership made up of U.S. and German promoters offers investors on the Internet what seems like a good deal — an opportunity to buy shares in a new, fast-growing company that promises returns of up to 420 percent annually. The partnership raises over \$1 million by telling investors that their initial investments are backed by a major bank and guaranteed against loss. Unfortunately, no such bank exists, and the organizers of the scam are prosecuted and ordered to repay investors.

According to an official of the U.S. Securities and Exchange Commission (SEC), cases of securities law violations like this are increasing in frequency as Internet usage swells and an increasing number of people use the medium to purchase securities and make investments.

A recent survey reports that the number of U.S. households with access to the Internet more than doubled to 14.7 million in 1996. The explosive growth in Internet usage has also created fantastic opportunities in the areas of securities, investments, and commerce. Investors can communicate with almost every conceivable market participant and find libraries of information about companies — all at little cost, and from the comfort of their own homes.

Forrester Research, a Cambridge, Massachusetts, consulting firm, predicts that the number of online accounts will grow from 1.5 million in 1996 to 10 million in 2001. According to the American Association of Individual Investors, 33 brokerage firms now offer some form of online trading, up from only 12 in 1995.

However, John Reed Stark, special counsel for Internet projects at the SEC's Division of Enforcement, said in a interview that the dramatic growth in online investing has a dark side to it — crooks and thieves looking for opportunities to rip-off unsuspecting investors.

"In light of the wide range of largely unregistered investment opportunities offered over the Internet, the SEC is well aware of the use of the Web as a convenient means for scam artists to steal from investors," Stark said. "The SEC has brought a host of cases thus far involving offerings over the Internet."

At very little cost and from the privacy of a basement office or living room, a fraudster can produce a home page that looks better than that of a Fortune 500 company. Thieves can even provide

a link to the home page of the SEC next to a representation that a particular security has received "approval" from the SEC.

Or a scam artist, called a "spammer" in this case, can pull a list of users from newsgroups catering to investors, send them the latest news about the "hottest" new investment, and direct them to a Web site or to a toll-free telephone number. In this way, with very little effort of time or money, the scam artist can reach an unlimited number of potential victims. Spammers combine the skills of mass mailers with the hard-pressure sales tactics of telephone pitchmen.

"Internet spammers have free rein to send information about bogus investment products to anyone with a modem, whether they like it or not," Stark said. "While there's no way to physically stop them from doing this, we can still prosecute them and shut down their Web sites."

Or a swindler might intercept the E-mail of an official of a public company, alter it by adding false information, and send it on to millions of people instantly in an attempt to manipulate the price of a stock.

"Like cat burglars who creep in without ever being seen," Stark said, "stock manipulators can steal an identity and make it their own, only the cyber-cat burglars need not climb up the drain pipe for a break-in or even don ski masks to hide their identities".

Stark said that the biggest concern right now are financial services offered over the Internet by foreign brokers, dealers, and investment advisers because they are so difficult to prosecute. Working from their home countries, foreign broker-dealers can vend their services to U.S. investors without ever crossing a border. While their activities may be legitimate in their own countries, they often violate strict registration and other provisions of the U.S. Securities Exchange Act of 1934.

"The entire area has become a massive can of worms," Stark said. "Given the many problems associated with investigating and prosecuting offshore entities, from serving subpoenas to locating assets to extradition, international

authorities must work together, using present treaties, memoranda of understanding, and other formal and informal international agreements."

As for what the SEC is doing to protect Internet investors, Stark is quick to point out that the commission has sought no new statutes, regulations, or rules to catch and prosecute those who commit Internet securities violations, and that Congressional intervention appears unnecessary.

"The swindles over the Internet are no different from the confidence games of the past," he said. "The only difference is the medium. Thus, present antifraud weapons will more than suffice. For instance, the antifraud provisions of the Securities Exchange Act of 1934 would apply to any fraudulent communication over the Internet, just as they apply to any information communicated on paper, or over the radio or television."

To track down the scam artists, the SEC uses a multifaceted approach that includes surveillance, education, and self-policing by individual Internet users. As part of its surveillance effort, Stark's division at the SEC employs the latest browsing software for viewing the Internet together with powerful hardware such as Pentium processors. The SEC also recently formed the "Cyberforce," a group of volunteers who spend several hours each week "surfing" the Web in search of securities law violations.

Stark's division has also set up a Website called the "Enforcement Complaint Center" — located as a link on the SEC home page — allowing Internet users to contact the SEC directly if they suspect wrongdoing. The site receives about 50 messages a day — more than 75 percent of which are useful for SEC investigations or referrals. The Enforcement Complaint Center can be found at the following Internet address:
<http://www.sec.gov/enforce/comctr.htm>.

"There exists a remarkable Internet culture of self-policing by individual users who resent the intrusion of the crooks and thieves trying to exploit the Internet," Stark said. "The division hopes to tap into this culture, encouraging users to report dubious offerings on the Web."

In the area of education, the SEC publishes the so-called Investor Alert, which contains an analysis of the types of online investment fraud and abuse together with suggestions for investors on how to avoid becoming the next victim. The alert even provides a checklist of steps to follow before making an investment over the Internet.

The SEC has also set up an online database, called EDGAR (<http://www.sec.gov/edgarhp.htm>), which provides the quarterly reports and management statements of companies, and is updated daily. The SEC hopes that EDGAR will help reduce the manipulation of share prices by giving investors access to the latest information.

Given the breadth of illicit activities on the Internet, Stark's division coordinates its policing efforts with other law enforcement agencies, including the U.S. Department of Justice, the Federal Bureau of Investigation, the Federal Communications Commission, the Federal Trade Commission, and a range of other civil and criminal law enforcement authorities.

Last December, the SEC teamed up with three other federal agencies and local law enforcement officials from 24 states to sponsor "Surf Day," which resulted in the identification of more than 500 possible cyberscams.

According to Stark, companies involved in offering or trading securities over the Internet must provide the same customer protections often taken for granted in the traditional trading of securities, such as with a registered U.S. exchange. These protections should mandate: (1) that investors' funds and securities are handled appropriately; (2) that investors understand the risks involved in purchasing the often illiquid and speculative securities that are traded over the Internet; (3) that buyers be made aware of the last sale prices on a particular stock; and (4) that companies provide on-going and adequate disclosure.

Jim Fuller writes on information technology and other global issues for the United States Information Agency.



THE INTERNET AND GLOBAL TRADE

By Harold Wolhandler
Director of Research
ActivMedia, Inc.

The Internet Today

The Internet has been tremendously successful. In the less than four years since opening its door to commercial growth, the Internet has blossomed into a vibrant marketplace. More than a third of a million active commercial Websites conducted an estimated \$24,400 million dollars of trade during 1997, according to a study we did at ActivMedia ("The Real Numbers Behind Net Profits 1997").

Nearly three-fourths of that trade was by companies based in the United States, but rapid expansion by European and Asia-Pacific corporations promises to spread the benefits of the Net around the world. No area has been left out. China, countries in South America, Africa, and elsewhere are now exploring ways to introduce Net activity consistent with their cultures and political climates.

There are eight primary requirements for the continued success and rapid expansion of today's Internet:

- A network with a common addressing system that can physically connect a multitude of computer resources.

- An intuitive graphical browser interface capable of point-and-click simplicity so that hardware and software tools would remove the burden of finding and extracting desired information.

- A marketplace of such organizational agents as search engines, directory trees, and database resources to organize the located information and provide links to direct traffic to the intended destination sites.

- A market approach to financing the Internet that acknowledges the vital role of central organizing processes to establish standards and promote inter-connectivity, yet recognizes the importance of stimulating free-market support for a public World Wide Web that can carry out commerce successfully.

- Governmental policies encouraging free or minimally regulated trade.

- Governmental policies supporting international copyright law.

- Governmental policies allowing free flow of public information.

- Adoption of global authentication standards.

Development is proceeding on several fronts. Initially an English language phenomenon, the Internet is now seeing around the globe the emergence of strong local-language structures aided by local-language directories and search tools.

Where local populations of Internet users have become large, online businesses have focused sales efforts at them, such as business-to-business services, financial products, consumer products, and entertainment, as well as local language directories and search tools to organize local content.

In a few areas with the greatest concentration of Internet users, online local business offerings extend to take-out foods with home delivery, restaurant and personal care reservations, grocery shopping with home delivery, and automotive repairs, including pickup and delivery of one's automobile.

Trade at A Distance

The increasingly transparent and liquid nature of global communications via the Internet is spurring world trade. The Internet has transformed our communication patterns from locally oriented to global networks where distance is invisible to users. In a sense, the geometry of our communication distance has diminished to near

zero, fostering long-distance relationships to every hopeful entrepreneur who establishes an Internet site.

The outgrowth of purchasing at a distance has transformed the shipping industry — not by the growth of new transportation vehicles, but by adding a wrapper of pure information to each shipment that coordinates the flow of merchandise among the trucks, trains, planes, and ships that handle goods.

Industry by industry, accelerated reliance on information is transforming relationships among companies and customers. This new set of relationships, in turn, is fostering new institutions able to meet the new needs of a globally communicating planet.

Risk and the Promise of Authentication

However easy it may be to place an order to a company halfway around the world, traditional risks of long-distance purchasing have not gone away. In fact, they have grown. Distance and the added cost of transportation serve to increase a host of risks, while simultaneously reducing the ability to easily resolve the difficulties that inevitably arise. It is this situation that authentication technologies seek to address in a number of ways.

Current online transaction security is usually limited to the transmission of encrypted data

Levels of Security and Authentication:

Password/Challenge — registration/trust based on first transaction.

Secure Forms Transmission — encrypts content during Internet passage.

Dual-Key Encryption — ensures that only intended recipient can open message. Parties pass encryption keys to each other.

Authentication — trusted third party issues digital certificates to known parties, reviews real-time transactions, provides key to valid merchant recipient to decrypt transmission, certifies that transaction occurred between buyer and seller with independent record of transactions.

Secure Electronic Transaction (SET) — common protocol for authentication services, allows multiple issuers of digital certificates to cooperate on transaction, integrates credit/debit/smart card clearing services with authentication service. It does not reveal card information to merchant.

between computers. Secure forms of data encryption, when combined with the growing skills of merchants at presenting merchandise online and at conducting electronic commerce, are sufficient for today's online business.

However, only one in seven online merchants currently reports that most of its orders are placed using encryption technologies. While almost half of all online merchants would like to conduct business directly on the Internet, most reported in our study that purchasers continue to place orders through traditional means — toll-free telephone numbers, faxed orders, and follow-up sales calls.

Apart from cases where products require final personal negotiation, the primary reason why most Internet-generated transactions are actually concluded offline appears to be lack of confidence in the systems and merchants involved in the transaction. A personal contact provides assurance to buyers that the company behind the Internet site really exists and stands ready to perform.

The risks involved in online commerce are both real and perceived. Customers have no way of knowing whether an online business is reliable — whether, in fact, the merchant Internet site they're visiting was not established to cheat them of their money.

Long distances may encourage careless non-performance by less-than-reputable online merchants. There is also the fear that transmissions routed through many computers may be intercepted and redirected, although this can happen only rarely. And finally, information residing on the merchant's computer (e.g. credit/debit card numbers) may be vulnerable to theft.

Merchants face similar risks — buyers denying that they placed an order, refusing to make payment, or making payment with false or stolen credit card numbers. No wonder people are uneasy about conducting commercial transactions on the Internet.

Authentication and the involvement of trusted third-party intermediaries promise to play an important role in reducing long-distance risk to buyers and sellers. A consortium of leading global

corporations and banks involved in credit cards and electronic commerce is nearing conclusion of a Secure Electronic Transaction (SET) protocol. This will:

- Issue "digital certificates" to known consumers that certify their identities when they punch in personal ID numbers at times of transaction;
- Retain a central repository of certificates that can be updated as circumstances warrant (revocation, new certificate issuance, etc.);
- Offer online merchants a means to clear credit/debit/smart card transactions in real-time through merchant bank accounts;
- Certify the identity of the online merchant to the buyer.

In addition, the protocol calls for encrypted transmission of order information, and, upon verifying and approving a transaction, it notifies the merchant that a sale has been approved and accounts have been credited. Merchants receive verification that orders are placed by authentic customers and have not been tampered with in transmission.

The merchant banks receive decrypted credit/debit/smart card information, but not actual details of the purchase, while merchants receive purchase approvals, but not actual credit card numbers. Close control of information on a "need-to-know" basis reduces the risk to all three parties to the transaction.

The result of SET will be that parties to a transaction will have at least a minimal level of confidence that the persons they are dealing with are who they represent themselves to be.

Beyond Cards — Larger Transactions

Purchases made with credit/debit/smart cards account for only a small fraction of all business conducted today. Most business transactions are conducted between known trading partners who offer traditional payment terms and extended credit lines. The potential for authentication and verification to enhance these traditional business transactions is similarly large.

As new communication abilities give rise to new institutions, we can expect to see information-based transaction support services using the tools of authentication and "trusted third party" services to support extended transactions of various kinds.

So-called assurance companies will find ways to lower transaction risks for buyers and sellers throughout the value chain. Their services will add value and growth to global trade and allow partnerships to form between parties who would never have dared to trade in a less information-intensive environment.

Hybrid transaction-support technologies that may appear include:

- Extended transaction plus delivery authentication. The integration of online credit approval with shipment-delivery proof can permit charging a buyer's account at time of sale, but holding payment in escrow until carriers submit authenticated proofs of shipment.
- Automated bill presentment. The secure submission of bills to individual and business accounts for later payment processing ensures that bills are presented in a timely fashion. Automated payment systems ease consumer burden for payment approval (an on-screen check-list), and instant status reports are available to vendors and consumers regarding open accounts.
- Guarantee and third party endorsement. A well-known neutral party provides assurances and guarantees that merchants it endorses will perform as specified (already offered by the Excite search engine).
- Authentication plus credit services. For orders shipped on credit, this combines knowledge of the purchaser with credit information supplied by banks and third-party services to establish lines of credit in real-time for inbound orders. This also automatically provides vendor access to customer credit information during order submission.
- Transnational extended transaction plus delivery authentication plus customs clearance. Adding an information wrapper to the actual shipment, as well as to the transaction, can reduce payment risk

through escrowing (an electronic letter of credit instrument), offering shipping insurance (specific to contents), providing customs clearance and tariff information (with "reply-button" ability to quickly contact freight originator to resolve difficulties), and tracking shipment progress and delivery (with alerts on delays, and release of escrow funds on delivery).

It is estimated that current paper-based systems of letters of credit, performance bonds, and insurance add as much as 20 percent to the cost of American manufactured goods. A comprehensive authentication/tracking/import-export system may dramatically reduce the risk-related economic burden and increase exports and imports.

- Transnational guarantee and third party endorsement. Authentication measures enable banks and trading partners in advance of a sale to convey cross-party assurances of performance and standardized and pre-agreed methods for problem resolution.

Information Authorization

Some information is inherently valuable. In the "smart home" of the future, video-telephones will be commonplace, and global authentication will be secured not by digital certificates, but by such personal physical characteristics such as retinal scans and palm-prints.

Computer-mediated communications allow any person to connect with any other person by cell-phone or computer screen. Unlimited personal reach will call for a new level of privacy control — communication access limited to voice until the recipient permits visual access as well. Authenticated parties (e.g., parents, children, employees) may be granted routine unlimited access.

Remote monitors will forward ringing doorbells to the away home or business owner and allow them to observe and speak with visitors even when not physically in the building.

Remote authorization may check with service companies to authenticate service-staff identity prior to authorizing remote door locks to open, and it may include cameras to observe and record

the visit, and later notify owners that the visitor has departed. This scenario is a small step from today's security minded systems, and portions of it are already in use today.

The potential for remote sensing and operation of all kinds has opportunities to enrich our lives. Medical consultations with specialists located thousands of kilometers away are already occurring.

Someday soon top-level surgeons may be performing remote operations thousands of kilometers from the operating room. Authentication will be imperative in cases like this.

What is left to follow? Maybe the remote manufacturing of custom goods, much like the Starship Enterprise's "replicators", where only the information required to manufacture an item is transmitted. Goods are fabricated locally, and authentication allows the sender to acknowledge actual manufacture (vs. onscreen preview of the product), and to charge and receive payment for information presented.

Global Implications and Benefits

Our small world grows smaller as we bridge time and space to conduct business worldwide. The new institutions that will rise to support our increasingly connected world will serve the advantaged and disadvantaged parts of the globe.

Lesser-developed areas will have access to developed-world products and services, and they will be able to present merchandise to compete in developed-world markets. Access to developed-world culture, knowledge, and service will boost development through better economic decisions wrought by more available information.

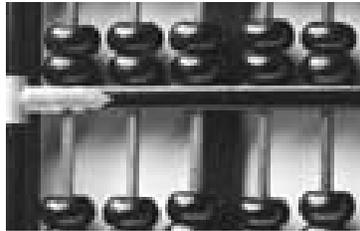
The risk-based limitations to doing business at a distance can be reduced through real-time information that is technically feasible. This includes new services such as authentication and validation and buyer and merchant endorsement by third-party insurers and financiers.

Efficient, sophisticated real-world delivery systems are the keys that can unlock an expanded potential for global trade. A global future lies before us.

*Harold Wolhandler's e-mail address is:
hwolhandler@ActivMedia.com.*

*ActivMedia of Peterborough, New Hampshire, has been tracking electronic commerce over the Internet through its global studies. ActivMedia's Web site is located at:
<http://www.ActivMedia.com>*

REPORTS AND DOCUMENTS



A FRAMEWORK FOR GLOBAL E-COMMERCE

The United States issued a report July 1, 1997, on global electronic commerce, setting forth general principles for a world-wide, free-trade zone on the Internet.

Among the principles outlined in the report, "A Framework for Global Electronic Commerce," are:

- The private sector should lead.
- Governments should avoid undue restraint on electronic commerce.
- Where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.

The full report can be found on the Internet at:
<http://www.iitf.nist.gov/elecomm/ecom.htm>

EXECUTIVE SUMMARY OF E-COMMERCE REPORT

The Internet has the potential to become the United States' most active trade vehicle within a decade, creating millions of high paying jobs. In addition, Internet shopping may revolutionize retailing by allowing consumers to sit in their

homes and buy a wide variety of products and services from all over the world.

Many businesses and consumers are wary of conducting extensive business electronically, however, because the Internet lacks a predictable legal environment governing transactions and because they are concerned that governments will impose regulations and taxes that will stifle Internet commerce.

A Framework for Global Electronic Commerce outlines the administration's strategy for fostering increased business and consumer confidence in the use of electronic networks for commerce. The paper reflects widespread consultation with industry, consumers groups, and the Internet community.

The paper presents five principles to guide government support for the evolution of electronic commerce and makes recommendations about nine key areas where international efforts are needed to preserve the Internet as a non-regulatory medium, one in which competition and consumer choice will shape the marketplace. With respect to these areas, the paper designates lead U.S. government

agencies and recommends international fora for consideration of each issue.

Principles

1. The private sector should lead. The Internet should develop as a market-driven arena not a regulated industry. Even where collective action is necessary, governments should encourage industry self-regulation and private sector leadership where possible.
2. Governments should avoid undue restrictions on electronic commerce. In general, parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. Governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or new taxes and tariffs on commercial activities that take place via the Internet.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable minimalist, consistent, and simple legal environment for commerce; where government intervention is necessary, its role should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, and facilitate dispute resolution, not to regulate.
4. Governments should recognize the unique qualities of the Internet. The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. Accordingly, the regulatory frameworks established over the past 60 years for telecommunication, radio, and television may not fit the Internet. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.
5. Electronic commerce on the Internet should be facilitated on a global basis. The Internet is a global marketplace. The legal framework supporting commercial transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller reside.

Recommendations

The principles described above guide the following recommendations:

1. **Tariffs and Taxation.** The Internet should be declared a tariff-free environment whenever it is used to deliver products and services. The Internet is a truly global medium, and all nations will benefit from barrier-free trade across it.

No new taxes should be imposed on Internet commerce. Existing taxes that are applied to electronic commerce should be consistent across national and sub-national jurisdictions and should be simple to understand and administer. State and local governments should cooperate to develop a uniform, simple approach to the taxation of electronic commerce, based on existing principles of taxation.

2. **Electronic Payment Systems.** The commercial and technological environment for electronic payments is changing rapidly, making it difficult to develop policy that is both timely and appropriate. For these reasons, inflexible and highly prescriptive regulations and rules are inappropriate and potentially harmful. In the near-term, case-by-case monitoring of electronic payment experiments is preferable to regulation.

3. **Uniform Commercial Code for Electronic Commerce.** In general, parties should be able to do business with each other on the Internet under the terms and conditions they agree upon. Private enterprise and free markets have typically flourished, however, where there are predictable and widely accepted legal principles supporting commercial transactions.

The United States supports the development of an international uniform commercial code to facilitate electronic commerce. Such a code should encourage governmental recognition of electronic contracts; encourage consistent international rules for acceptance of electronic signatures and other authentication procedures; promote the development of alternative dispute resolution mechanisms for international commercial transactions; set predictable ground rules for exposure to liability; and streamline the use of electronic registries.

4. Intellectual Property Protection. Commerce on the Internet will often involve the sale and licensing of intellectual property. To promote electronic commerce, sellers must know that their intellectual property will not be stolen and buyers must know that they are obtaining authentic products. Clear and effective copyright, patent, and trademark protection is therefore necessary to protect against piracy and fraud.

The recently negotiated World Intellectual Property Organization (WIPO) treaties for copyright protection should be ratified. Issues of liability for infringement, application of the fair use doctrine, and limitation of devices to defeat copyright protection mechanisms should be resolved in a balanced way, consistent with international obligations.

The government will study and seek public comment on the need to protect database elements that do not qualify for copyright protection and, if such protection is needed, how to construct it.

The administration will promote global efforts to provide adequate and effective protection for patentable subject matter important to the development of the Global Information Infrastructure (GII), and establish standards for determining the validity of patent claims.

The administration also will work globally to resolve conflicts that arise from different national treatments of trademarks as they relate to the Internet. It may be possible to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis.

The administration will review the system of allocating domain names in order to create a more competitive, market-based system and will seek to foster bottom-up governance of the Internet in the process.

5. Privacy. It is essential to assure personal privacy in the networked environment if people are to feel comfortable doing business across this new medium.

Data gatherers should tell consumers what information they are collecting and how they

intend to use it. Consumers should have meaningful choice with respect to the use and re-use of their personal information. Parents should be able to choose whether or not personal information is collected from their children. In addition, redress should be available to consumers who are harmed by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information.

The administration supports private sector efforts now underway to implement meaningful, user friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, private sector adoption of and adherence to fair information practices, and dispute resolution. The government will work with industry and privacy advocates to develop appropriate solutions to privacy concerns that may not be fully addressed by industry through self-regulation and technology.

6. Security. The GI must be secure and reliable. If Internet users do not believe that their communications and data are safe from interception and modification, they are unlikely to use the Internet on a routine basis for commerce. The administration, in partnership with industry, is taking steps to promote the development of a market-driven public key infrastructure that will enable trust in encryption and provide the safeguards that users and society will need.

7. Telecommunications Infrastructure and Information Technology. Global electronic commerce depends upon a modern, seamless, global telecommunications network and upon the "information appliances" that connect to it. In too many countries, telecommunications policies are hindering the development of advanced digital networks. The United States will work internationally to remove barriers to competition, customer choice, lower prices, and improved services.

8. Content. The administration encourages industry self-regulation, the adoption of competitive content rating systems, and the development of effective, user-friendly technology tools (e.g., filtering and blocking technologies) to

empower parents, teachers, and others to block content that is inappropriate for children.

The government will seek agreements with our trading partners to eliminate overly burdensome content regulations that create non-tariff trade barriers.

9. **Technical Standards.** The marketplace, not governments, should determine technical standards and other mechanisms for inter-operability on the Internet. Technology is moving rapidly and governments' attempts to establish technical standards to govern the Internet would only risk inhibiting technological innovation.

Coordinaton

The administration will continue to coordinate its approach to electronic commerce. The interagency team that developed this framework and strategy will continue to meet to update the strategy and facilitate its implementation as events unfold.

Background on President's Memorandum for Department and Agency Heads

The president today issued a memorandum for the heads of all executive branch departments and agencies directing them to implement the strategy outlined in A Framework for Global Electronic Commerce.

The memorandum first instructs executive branch officials to apply the framework's five basic principles to any actions they take with respect to electronic commerce. These principles call for the Internet to function as a market-driven environment with minimal government regulation, and for the Internet to be governed by a consistent set of rules across state, national, and international borders.

The memorandum then lists 13 specific objectives and designates appropriate executive branch officers to head government efforts to achieve these objectives. In several cases, the memorandum directs executive branch officers to achieve specific objectives within the next 12 months.

1. The memorandum directs the U.S. Trade Representative to secure international agreement

within the next 12 months to reduce tariffs on Internet-related equipment to zero and to ensure that products and services delivered across the Internet are not subject to tariff.

2. The memorandum directs the secretary of commerce to seek domestic and international agreement within the next 12 months on common approaches for the authentication of electronic transactions through technologies such as digital signatures.

3. The memorandum directs the secretary of commerce and the director of the Office of Management and Budget to encourage private sector development and deployment within the next 12 months, of effective, industry-developed codes of conduct and technology tools to protect privacy online, especially with respect to children.

4. The memorandum directs the secretary of commerce to encourage the development of user-friendly filtering technologies and private rating systems within the next 12 months that empower parents, teachers, and other Internet users to block content that they deem inappropriate for their children.

5. The memorandum directs the secretary of the treasury to work with domestic and foreign government officials to assure that no new taxes are imposed on Internet commerce and that existing taxes are applied in ways which do not hinder nor distort commerce.

6. The memorandum directs the administrator of the General Services Administration to bring federal government purchasing into the electronic age by arranging for federal purchasing of four million items online within the next 12 months.

7. The memorandum directs the secretary of commerce to support efforts to establish a private, competitive system for allocating domain names and to create a contractually based, self-regulatory regime to resolve conflicts between domain name usage and trademark laws globally.

8. The memorandum directs the secretary of treasury to work domestically and internationally to ensure that no new taxes are imposed on Internet commerce, that existing taxes are

technology neutral and avoid inconsistent tax jurisdiction and double taxation problems.

9. The memorandum directs the secretary of commerce to work globally to support development of a "Uniform Commercial Code" for cyberspace that recognizes, facilitates, and enforces electronic agreements worldwide.

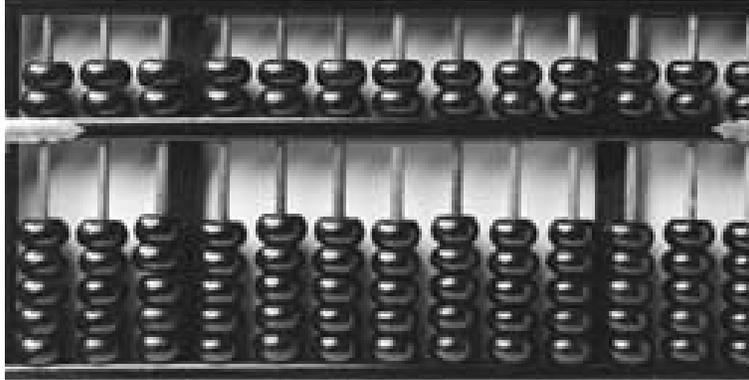
10. The memorandum directs the secretary of commerce to support private sector development of technical standards for the Internet and direct the U.S. Trade Representative to oppose governmental efforts to mandate standards or use standards as non-tariff trade barriers.

11. The memorandum directs the secretary of treasury to monitor emerging electronic payment technology, to oppose government efforts to regulate electronic payment at this time, and to work with the private sector to ensure that any necessary government activity in this area can flexibly accommodate the needs of the emerging marketplace.

12. The memorandum directs all agencies to work domestically and internationally to make the Internet a secure environment for commerce, supported by a robust infrastructure, and well-trained Internet users who understand how to protect their systems and their data.

13. The memorandum directs the secretary of commerce to enhance the ability of our patent system to protect patentable innovations in the electronic age, and to work to ensure that patentable subject matter important to global commerce is protected globally.

The memorandum establishes an interagency group under the leadership of the vice president to coordinate implementation of the government's strategy for electronic commerce and directs agency heads to report to him through the interagency group every six months on progress towards meeting all of the specific objectives outlined in the memorandum.



THE END OF NATIONAL MARKETS

by Stephen J. Kobrin

Twenty-six years ago, Raymond Vernon's "Sovereignty at Bay" proclaimed that "concepts such as national sovereignty and national economic strength appear curiously drained of meaning."

Other books followed, arguing that sovereignty, the nation-state, and the national economy were finished — victims of multinational enterprises and the internationalization of production. While sovereign states and national markets have outlasted the chorus of Cassandras, this time the sky really may be falling. The emergence of electronic cash and a digitally networked global economy pose direct threats to the very basis of the territorial state.

Let us begin with two vignettes. Fact: Smugglers fly Boeing 747s loaded with illicit drugs into Mexico and then cram the jumbo jets full of cash — American bills — for the return trip. Fiction: Uncle Enzo, Mafia CEO, pays for intelligence in the digital future of Neal Stephenson's novel *Snow Crash*: "He reaches into his pocket and pulls out a hypercard and hands it toward Hiro. It says 'Twenty-Five Million Hong Kong Dollars.' Hiro reaches out and takes the card. Somewhere on earth, two computers swap bursts of electronic

noise and the money gets transferred from the Mafia's account to Hiro's."

The 747s leaving Mexico are anachronisms, among the last surviving examples of the physical transfer of large amounts of currency across national borders. Most money has been electronic for some time. Virtually all of the trillions of dollars, marks, and yen that make their way around the world each day take the form of bytes — chains of zeros and ones. Only at the very end of its journey is money transformed into something tangible: credit cards, checks, cash, or coins.

Hypercards are here. Mondex, a smart card or electronic purse, can be "loaded" with electronic money from an automatic teller machine (atm) or by telephone or personal computer using a card-reading device. Money is spent either by swiping the card through a retailer's terminal or over the Internet by using the card reader and a personal computer. An electronic wallet allows anonymous card-to-card transfers.

Copyright (c) 1997 Carnegie Endowment for International Peace. Reprinted with permission from FOREIGN POLICY magazine, Summer 1997.

It is not just the current technology of electronic cash (e-cash) or even what might be technologically feasible in the future that presents policymakers with new challenges. Rather, policymakers must confront directly the implications of this technology — and, more generally, the emergence of an electronically networked global economy — for economic and political governance. As the U.S. comptroller of the currency, Eugene Ludwig, has noted, "There is clearly a freight train coming down the tracks. Just because it hasn't arrived yet doesn't mean we shouldn't start getting ready."

Electronic Money

Many different forms of "electronic money" are under development, but it is useful to look at three general categories: electronic debit and credit systems; various forms of smart cards; and true digital money, which has many of the properties of cash.

Electronic debit and credit systems already exist. When a consumer uses an ATM card to pay for merchandise, funds are transferred from his or her account to the merchant's. Credit cards are used to make payments over the Internet. Computer software such as Intuit provides electronic bill payment, and it is but a short step to true electronic checks — authenticated by a digital signature — that can be transmitted to the payee, endorsed, and deposited over the Internet. Electronic debit and credit systems represent new, more convenient means of payment, but not new payment systems. A traditional bank or credit card transaction lies at the end of every transaction chain.

Smart cards and digital money represent new payment systems with potentially revolutionary implications. Smart cards are plastic "credit" cards with an embedded microchip. Many are now used as telephone or transit payment devices. They can be loaded with currency from an atm or via a card reader from a telephone or personal computer, which can then be spent at businesses, vending machines, or turnstiles that have been equipped with appropriate devices. At this most basic level, a smart card is simply a debit card that does not require bank approval for each transaction; clearance takes place each day and the value

resides in third-party accounts. There is no reason, however, that smart cards have to be limited in this way.

Banks or other institutions could provide value on smart cards through loans, payments for services, or products. The immediate transfer of funds between bank accounts is not necessary; units of value can circulate from card to card — and from user to user — without debiting or crediting third-party accounts. Assuming confidence in the creating institution, "money" could be created on smart cards and could circulate almost indefinitely before redemption.

Finally, electronic money can take true digital form, existing as units of value in the form of bytes stored in the memory of personal computers that may or may not be backed up by reserve accounts of real money. The money could be downloaded from an account, supplied as a loan or as payment, or bought with a credit card over the Internet. As long as digital cash can be authenticated and there is confidence in its continued acceptance, it could circulate indefinitely, allowing peer-to-peer payments at will. These are big "ifs," but they are well within the realm of the possible.

Imagine a world where true e-cash is an everyday reality. Whether all of the following assumptions are correct or even immediately feasible is unimportant; some form of e-cash is coming, and we need to begin the process of thinking about its as-yet-unexplored consequences for economic and political governance.

The year is 2005. You have a number of brands of e-cash on your computer's hard drive: some withdrawn from a bank in Antigua, some borrowed from Microsoft, and some earned as payment for your services. You use the digital value units (DVUs) to purchase information from a Web site, pay bills, or send money to your daughter in graduate school. Peer-to-peer payments are easy: You can transfer DVUs to any computer anyplace in the world with a few keystrokes.

Your e-cash is secure and can be authenticated easily. It is also anonymous; governments have not been able to mandate a technology that leaves a clear audit trail. Public-key encryption technology

and digital signatures allow blind transactions; the receiving computer knows that the DVUs are authentic without knowing the identity of the payer. Your e-cash can be exchanged any number of times without leaving a trace of where it has been. It is virtually impossible to alter the value of your e-cash at either end of the transaction (by adding a few more zeros to it, for example).

DVUs are almost infinitely divisible. Given the virtually negligible transaction cost, it is efficient

for you to pay a dollar or two to see a financial report over the Internet or for your teenager to rent a popular song for the few minutes during which it is in vogue. Microtransactions have become the norm. E-cash is issued — actually created — by a large number of institutions, bank and nonbank. Electronic currencies (e-

currencies) have begun to exist on their own; many are no longer backed by hard currency and have developed value separately from currencies issued by central banks. DVUs circulate for long periods of time without being redeemed or deposited. Consumer confidence in the issuer is crucial; as with electronic commerce (e-commerce) in general, brand names have become critical.

The early 21st century is described as a world of competing e-currencies, a throwback to the 19th-century world of private currencies. The better known brands of e-cash are highly liquid and universally accepted. It is a relatively simple matter for you to set up filters in your electronic purse to screen out e-currencies that you do not want to accept.

Government In The Digital World

E-cash and the increasing importance of digital markets pose problems for central government control over the economy and the behavior of economic actors; they also render borders around national markets and nation-states increasingly permeable — or, perhaps, increasingly irrelevant. In a world where true e-cash is an everyday reality, the basic role of government in a liberal market economy and the relevance of borders and geography will be drastically redefined.

While at first glance this concern appears to reflect a traditional break between domestic and international economic issues, in fact the advent of e-cash raises serious questions about the very idea of “domestic” and “international” as meaningful and distinct concepts. The new digital world presents a number of governance issues, described below.

- Can central banks control the rate of growth and the size of the money supply? Private e-currencies will make it difficult for central bankers to control — or even measure or define — monetary aggregates. Several forms of money, issued by banks and nonbanks, will circulate. Many of these monies may be beyond the regulatory reach of the state. At the extreme, if, as some libertarians imagine, private currencies dominate, currencies issued by central banks may no longer matter.

- Will there still be official foreign exchange transactions? E-cash will markedly lower existing barriers to the transfer of funds across borders. Transactions that have been restricted to money-center banks will be available to anyone with a computer. Peer-to-peer transfers of DVUs across national borders do not amount to “official” foreign exchange transactions. If you have \$200 worth of DVUs on your computer and buy a program from a German vendor, you will probably have to agree on a mark-to-dollar price. However, transferring the DVUs to Germany is not an “official” foreign exchange transaction; the DVUs are simply revalued as marks. In fact, national currencies may lose meaning with the development of DVUs that have a universally accepted denomination. Without severe restrictions on individual privacy — which are not out of the question — governments will be hard-pressed to track, account for, and control the flows of money across borders.

- Who will regulate or control financial institutions? The U.S. Treasury is not sure whether existing regulations, which apply to both banks and institutions that act like banks (i.e., take deposits), would apply to all who issue (and create) e-cash. If nonfinancial institutions do not accept the extensive regulatory controls that banks take as the norm, can reserve or reporting requirements be enforced? What about consumer protection in the event of the insolvency of an issuer of e-cash, a

**E-cash is
an
everyday
reality**

system breakdown, or the loss of a smart card?

- Will national income data still be meaningful? It will be almost impossible to track transactions when e-cash becomes a widely used means of payment, online deals across borders become much easier, and many of the intermediaries that now serve as checkpoints for recording transactions are eliminated by direct, peer-to-peer payments. The widespread use of e-cash will render national economic data much less meaningful. Indeed, the advent of both e-cash and e-commerce raises fundamental questions about the national market as the basic unit of account in the international economic system.

- How will taxes be collected? Tax evasion will be a serious problem in an economy where e-cash transactions are the norm. It will be easy to transfer large sums of money across borders, and tax havens will be much easier to reach. Encrypted anonymous transactions will make audits increasingly problematic. Additionally, tax reporting and compliance relies on institutions and intermediaries. With e-cash and direct payments, all sorts of sales taxes, value-added taxes, and income taxes will be increasingly difficult to collect. More fundamentally, the question of jurisdiction — who gets to tax what — will become increasingly problematic. Say you are in Philadelphia and you decide to download music from a computer located outside Dublin that is run by a firm in Frankfurt. You pay with e-cash deposited in a Cayman Islands account. In which jurisdiction does the transaction take place?

- Will e-cash and e-commerce widen the gap between the haves and the have-nots? Participation in the global electronic economy requires infrastructure and access to a computer. Will e-cash and e-commerce further marginalize poorer population groups and even entire poor countries? This widened gap between the haves and the have-nots — those with and without access to computers — could become increasingly difficult to bridge.

- Will the loss of seigniorage be important as governments fight to balance budgets? Seigniorage originally referred to the revenue or profit generated due to the difference between the cost

of making a coin and its face value; it also refers to the reduction in government interest payments when money circulates. The U.S. Treasury estimates that traditional seigniorage amounted to \$773 million in 1994 and that the reduction in interest payments due to holdings of currency rather than debt could be as much as \$3.5 billion per year. The Bank for International Settlements reports that the loss of seigniorage for its 11 member states will be more than \$17 billion if smart cards eliminate all bank notes under \$25.

- Will fraud and criminal activity increase in an e-cash economy? At the extreme — and the issue of privacy versus the needs of law enforcement is unresolved — transfers of large sums of cash across borders would be untraceable. There would be no audit trail. Digital counterfeiters could work from anywhere in the world and spend currency in any and all places. New financial crimes and forms of fraud could arise that would be hard to detect, and it would be extremely difficult to locate the perpetrators. The task of financing illegal and criminal activity would be easier by orders of magnitude. E-cash will lower the barriers to entry and reduce the risks of criminal activity.

Most of the issues raised in the recent National Research Council report on cryptography's role in the information society apply directly to electronic cash. Secure, easily authenticated, and anonymous e-cash requires strong encryption technology. Anonymous transactions, however, cannot be restricted to law-abiding citizens. Encryption makes it as difficult for enforcement authorities to track criminal activity as it does for criminals to penetrate legitimate transmissions. Should privacy be complete? Or should law enforcement authorities and national security agencies be provided access to e-cash transactions through escrowed encryption, for example? What about U.S. restrictions on the export of strong encryption technology? E-cash is global cash; how can governments limit its geographic spread? Can they even suggest that strong encryption algorithms be restricted territorially?

Geographic Space Versus Cyberspace

A recent U.S. Treasury paper dealing with the tax implications of electronic commerce argues that new communications technologies have

**Disconnection
Between
E-Markets
and Political
Geography**

"effectively eliminated national borders on the information highway." It is clear from the paper's subsequent discussion, however, that the more fundamental problem is that electronic commerce may "dissolve the link between an income-producing activity and a specific location."

The source of taxable income, which plays a major role in determining liability, is defined geographically in terms of where the economic activity that produces the income is located. Therein lies the rub: "Electronic commerce doesn't seem to occur in any physical location but instead takes place in the nebulous world of 'cyberspace.'" In a digital economy it will be difficult, or even impossible, to link income streams with specific geographic locations.

Digitalization is cutting money and finance loose from its geographic moorings. The framework of regulation that governs financial institutions assumes that customers and institutions are linked by geography — that spatial proximity matters.

E-cash and e-commerce snap that link. What remains are systems of economic and political governance that are rooted in geography and are trying nonetheless to deal with e-cash and markets that exist in cyberspace. The obvious disconnect here will only worsen over time.

The geographical rooting of political and economic authority is relatively recent. Territorial sovereignty, borders, and a clear distinction between domestic and international spheres are modern concepts associated with the rise of the nation-state. Territorial sovereignty implies a world divided into clearly demarcated and mutually exclusive geographic jurisdictions. It implies a world where economic and political control arise from control over territory.

The international financial system — which consists of hundreds of thousands of computer screens around the globe — is the first international electronic marketplace. It will not be the last. E-cash is one manifestation of a global economy that is constructed in cyberspace rather

than geographic space. The fundamental problems that e-cash poses for governance result from this disconnect between electronic markets and political geography.

The very idea of controlling the money supply, for example, assumes that geography provides a relevant means of defining the scope of the market. It assumes that economic borders are effective, that the flow of money across them can be monitored and controlled, and that the volume of money within a fixed geographic area is important. All of those assumptions are increasingly questionable in a digital world economy.

Many of our basic tax principles assume that transactions and income streams can be located precisely within a given national market. That assumption is problematic when e-cash is spent on a computer network. It is problematic when many important economic transactions cannot be located, or may not even take place, in geographic space.

The increasing irrelevance of geographic jurisdiction in a digital world economy markedly increases the risks of fraud, money-laundering, and other financial crimes. Asking where the fraud or money-laundering took place means asking "Whose jurisdiction applies?" and "Whose law applies?" We need to learn to deal with crimes that cannot be located in geographic space, where existing concepts of national jurisdiction are increasingly irrelevant.

The term "disintermediation" was first used to describe the replacement of banks as financial intermediaries by direct lending in money markets when interest rates rose. It is often used in the world of e-commerce to describe the elimination of intermediaries by direct seller-to-buyer transactions over the Internet. Many observers argue that e-cash is likely to disintermediate banks. Of more fundamental importance is the possibility that e-cash and e-commerce will disintermediate the territorial state.

To be clear, I argue that we face not the end of the state, but rather the diminished efficacy of political and economic governance that is rooted in geographic sovereignty and in mutually exclusive

territorial jurisdiction. Questions such as: "Where did the transaction take place?" "Where did the income stream arise?" "Where is the financial institution located?" and "Whose law applies?" will lose meaning.

E-cash and e-commerce are symptoms, albeit important ones, of an increasing asymmetry between economics and politics, between an electronically integrated world economy and territorial nation-states, and between cyberspace and geographic space. How this asymmetry will be resolved and how economic and political relations will be reconstructed are two of the critical questions of our time.

What is to be done

The question asked here is not "What is feasible?" but "What are the limits of the possible?" Whether the picture presented here is correct in all — or even some — of its details is unimportant. A digital world economy is emerging. Imagining possible scenarios is necessary if we are to come to grips with the consequences of this revolution.

The purpose here is to raise problems rather than to solve them and to imagine possible futures and think about their implications for economic and political governance. A digital world economy will demand increasing international cooperation, harmonizing national regulations and legislation, and strengthening the authority of international institutions.

The harmonization of national regulations will help to prevent institutions, such as those issuing e-cash, from slipping between national jurisdictions or shopping for the nation with the least onerous regulations. However, it will not

address the basic problem of the disconnect between geographic jurisdiction and an electronically integrated global economy. If it is impossible to locate transactions geographically — if the flows of e-cash are outside of the jurisdictional reach of every country — then the harmonization of national regulations will accomplish little. The basic problem is not one of overlapping or conflicting jurisdictions; it stems from the lack of meaning of the very concept of "jurisdiction" in a digitalized global economy.

The erosion of the viability of territorial jurisdiction calls for strengthened international institutions. It calls for giving international institutions real authority to measure, to control, and, perhaps, to tax. The Basle Committee on Banking Supervision — an international body of bank regulators who set global standards — could perhaps be given the authority to collect information from financial institutions wherever they are located and formulate and enforce regulations globally. Interpol, or its equivalent, may have to be given jurisdiction over financial crimes, regardless of where they are committed. That does not mean a world government; it does mean a markedly increased level of international cooperation.

The questions we must face are whether territorial sovereignty will continue to be viable as the primary basis for economic and political governance as we enter the 21st century and what the implications will be for the American economy — and Americans in general — if we refuse to cooperate internationally in the face of an increasingly integrated global economy.

ELECTRONIC CASH: A GLOSSARY

DIGITAL DATA: Information coded into a series of zeros and ones that can be transmitted and processed electronically.

DIGITAL SIGNATURE: A code that allows absolute authentication of the origin and integrity of a document, check, or electronic cash that has been sent over a computer network. A blind signature allows authentication without revealing the identity of the sender.

DISINTERMEDIATION: The substitution of direct transactions for those that are mediated. The term

originated when rising interest rates caused savings to be withdrawn from banks — whose interest rates were capped — and invested in money market instruments that were the direct debts of borrowers. Banks were disintermediated. In electronic commerce, the term refers to the rise of direct buyer-to-seller relationships over the Internet, disintermediating wholesalers and retail outlets.

ELECTRONIC MONEY: Units or tokens of monetary value that take digital form and are transmitted over electronic networks. Digital Value Units are the basic units of denomination of electronic money; they may or may not correspond to units of national currency.

ENCRYPTION: The coding of information for security purposes, such as credit card numbers or electronic cash used over the Internet. Public-key encryption uses a mathematical algorithm comprising a pair of strings of numbers to encrypt and decrypt the data. For example, the sender would encrypt the data with the receiver's public key and the receiver would decrypt with his or her private key.

INTERNET: A global network of linked networks that allows communication and the sharing of information among many different types of computers. The World Wide Web is a graphical system on the Internet that allows rapid movement between documents and computers through the use of embedded (hypertext) links.

SMART CARDS: A plastic card, similar to a credit card, containing a microchip that can be used to retrieve, store, process, and transmit digital data like electronic cash or medical information.



Stephen J. Kobrin is the director of the Lauder Institute of Management and International Studies and the William Wurster professor of multinational management at the Wharton School of the University of Pennsylvania. This paper develops themes raised at a discussion of electronic money at the 1997 annual meeting of the World Economic Forum in Davos, Switzerland.

Permission has been obtained covering republication/translation/abridgment by USIS and the local press outside the United States.

DEPARTMENTS



Bibliography

BOOKS AND DOCUMENTS

Ahuja, Vijay.

SECURE COMMERCE ON THE INTERNET
Academic Press, 1996. 298p.

ELECTRONIC COMMERCE: OPPORTUNITIES AND CHALLENGES FOR GOVERNMENT

Organisation for Economic Co-operation and Development, 1997. 83p. Available on Internet at <http://www.oecd.org/dsti/pubs/SACHER.HTM>

A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE

The White House, 1997. 32p.
Available on Internet at <http://www.iitf.nist.gov/eleccomm/ecom.htm>

Group of Ten.

ELECTRONIC MONEY: CONSUMER PROTECTION, LAW ENFORCEMENT, SUPERVISORY AND CROSS BORDER ISSUES

Bank for International Settlements, 1997.45p.
Available on Internet at <http://www.bis.org/publ/gent.htm>

Haynes, Ted.

THE ELECTRONIC COMMERCE DICTIONARY: THE DEFINITIVE TERMS FOR DOING BUSINESS ON

THE INFORMATION SUPERHIGHWAY
Robleda Company, 1995. 128p.

Kalakota, Ravi; Whinston, Andrew.

ELECTRONIC COMMERCE: A MANAGER'S GUIDE
Addison-Wesley, 1997. 440p.

Kalakota, Ravi; Whinston, Andrew, eds.

READINGS IN ELECTRONIC COMMERCE
Addison-Wesley, 1997. 368p.

Keen, Peter G. W.; Ballance, Craig.

ON-LINE PROFITS: A MANAGER'S GUIDE TO ELECTRONIC COMMERCE
Harvard Business School Publishing, 1997. 304p.

Nemzow, Martin.

BUILDING CYBERSTORES: INSTALLATION, TRANSACTION PROCESSING, AND MANAGEMENT
McGraw-Hill, 1997. 522p.

Net.Genesis Corporation.

BUILD A WORLD WIDE WEB COMMERCE CENTER: PLAN, PROGRAM AND MANAGE INTERNET COMMERCE FOR YOUR COMPANY
John Wiley, 1996. 464p.

Tapscott, Don.

THE DIGITAL ECONOMY: PROMISE AND PERIL IN THE AGE OF NETWORKED INTELLIGENCE
McGraw-Hill, 1995. 342p.

U.S. Department of the Treasury.

AN INTRODUCTION TO ELECTRONIC MONEY ISSUES

U.S. Department of the Treasury, 1996. 60p.
Available on Internet at <http://www.occ.treas.gov/e-money/papinf.htm>

U.S. Department of the Treasury. Office of Tax Policy.

SELECTED TAX POLICY IMPLICATIONS OF GLOBAL ELECTRONIC COMMERCE

U.S. Department of the Treasury, 1996. 44p.
Available on Internet at <http://www.ustreas.gov/treasury/tax/internet.html>

ARTICLES

Brock, Terry; Yudkowsky, Chaim.

PURCHASING BOOKS ONLINE IS EASY, CONVENIENT AND FUN

(Dallas Business Journal, Vol. 20, May 30, 1997, p. B7+)

Camp, L. Jean; Sirbu, Marvin.

CRITICAL ISSUES IN INTERNET COMMERCE

(IEEE Communications Magazine, Vol. 35, No. 5, May 1997, pp. 58+)

Cella, Joseph J., III; Stark, John Reed.

SEC ENFORCEMENT AND THE INTERNET: MEETING THE CHALLENGE OF THE NEXT MILLENNIUM: A PROGRAM FOR THE EAGLE AND THE INTERNET

(The Business Lawyer, Vol. 52, No. 3, May 1997, pp. 815-832)

Childs, Kelvin.

WHITE HOUSE AND THE INTERNET

(Editor and Publisher, Vol. 130, No. 28, July 12, 1997, pp. 10-11)

Clark, Tanya.

ASIA WOBBLER ONTO THE WEB

(Industry Week, Vol. 246, No. 8, April 21, 1997, pp. 80+)

Cortese, Amy.

THE ULTIMATE PLASTIC

(Business Week, No. 3527, May 19, 1997, pp. 119, 122)

Gee, Jack.

PARLEZ-VOUS INTER-NET?

(Industry Week, Vol. 246, No. 8, April 21, 1997, pp. 78-79)

Hodges, Mark.

IS WEB BUSINESS GOOD BUSINESS?

(Technology Review, Vol. 100, No. 6, August/September 1997, pp. 22-28)

Jones, Chris.

END-TO-END INTERNET SECURITY STILL DEPENDS ON ENCRYPTION APPS

(InfoWorld, Vol. 19, No. 14, April 7, 1997, pp. 41-42)

Kobrin, Stephen J.

ELECTRONIC CASH AND THE END OF NATIONAL MARKETS

(Foreign Policy, No. 107, Summer 1997, pp. 65-77)

Lardner, Richard.

KEYS TO THE CODE

(Government Executive, Vol. 29, No. 7, July 1997, pp. 29-30, 32)

Marion, Larry.

WHO'S GUARDING THE TILL AT THE CYBERMALL?

(Datamation, Vol. 41, No. 3, February 15, 1995, pp. 38-39)

Mueller, Milton.

TELECOMMUNICATIONS ACCESS IN THE AGE OF ELECTRONIC COMMERCE: TOWARD A THIRD-GENERATION UNIVERSAL SERVICE POLICY

(Federal Communications Law Journal, Vol. 49, No. 3, April 1, 1997, pp. 655+)

Powell, Mark D.

ELECTRONIC COMMERCE: AN OVERVIEW OF THE LEGAL AND REGULATORY ISSUES

(International Trade Law and Regulation, Vol. 3, No. 3, June 1, 1997, pp. 85+)

Shapiro, Andrew L.

PRIVACY FOR SALE: PEDDLING DATA ON THE INTERNET

(Nation, Vol. 264, No. 24, June 23, 1997, pp. 11-16)

SURVEY: ON-LINE COMMERCE

(The Economist, Vol. 343, No. 8016, May 10, 1997, pp. E3-E18)

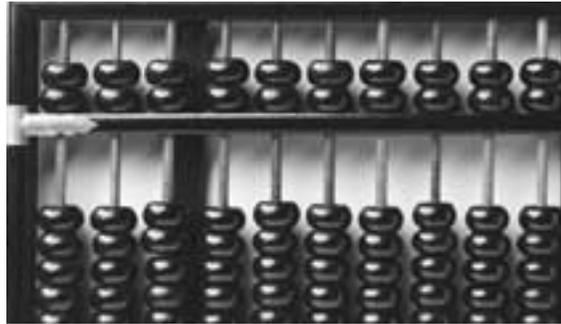
THEORY AND PRACTICE OF ELECTRONIC COMMERCE

(The Information Society, Vol. 13, No. 1, January-March 1997, Special Issue, pp. 1-145)

Tucker, Michael Jay.

THE NEW MONEY: TRANSACTIONS POUR ACROSS THE WEB

(Datamation, Vol. 43, No. 4, April 1997, pp. 73-76, 78)



Electronic Commerce: Key Internet Sites

WEB SITES

USIS assumes no responsibility for the content or availability of these sites

Cryptopography Policy

Electronic Privacy Information Center
<http://www.epic.org/crypto/>

Computer Security Resource Clearinghouse

National Institute of Standards and Technology
<http://csrc.nist.gov/>

Electronic Commerce Web Sites

Yahoo Search
http://www.yahoo.com/Business_and_Economy/Electronic_Commerce

Electronic Commerce in the National Information Infrastructure

Corporation for National Research Initiatives
http://www.xiwt.org/XIWT/documents/EComm_doc/ECommTOC2.html

Electronic Commerce Information Resource

<http://www.year-x.co.uk/ec/yxwhatis.htm>

Electronic Commerce Resource Guide

Premenos Corporation — software firm for electronic commerce
<http://www.premenos.com/Resources/main.html>

Electronic Commerce and the European Union

European Initiative in Electronic Commerce
<http://www.ispo.cec.be/Ecommerce>

Emergence of Electronic Commerce on the Internet

School of Business Administration, University of Southern California
http://www.usc.edu/dept/ATRIUM/Papers/EC_on_the_Inet.html

Foreign Investment In Emerging Markets

Sponsored by the Multilateral Investment Guarantee Agency
<http://www.ipanet.net/>

U.S. International Trade Statistics

U.S. Census Bureau
<http://www.census.gov/foreign-trade/www/>

Framework for Global Electronic Commerce

White House report
<http://www.iitf.nist.gov/eleccomm/ecomm.htm>

Office of the North American Free Trade Agreement

U.S. Department of Commerce

<http://www.itaiep.doc.gov/nafta/nafta2.htm>

Selected Tax Policy Implications of Global Electronic Commerce

Office of Tax Policy, Department of Treasury

<http://www.ustreas.gov/treasury/tax/internet.html>

Special Issue on Electronic Commerce

Journal of Computer-Mediated Communication

<http://www.usc.edu/dept/annenberg/vol1/issue3/vol1no3.html>

U.S. Government Statistics

Links to Federal Government statistics

<http://www.fedstats.gov/>

The Attention Economy and the Net

“First Monday” journal on the Internet

http://www.firstmonday.dk/issues/issue2_4/goldhaber/index.html

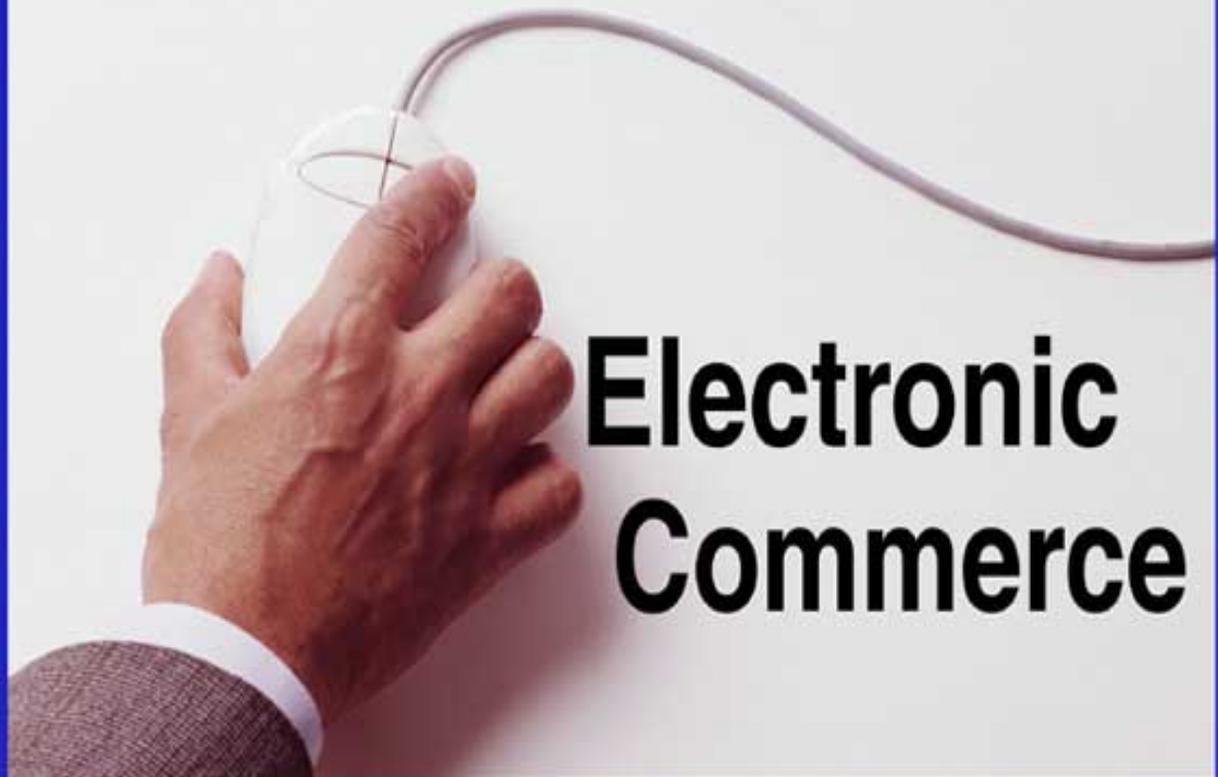
Telecom Information Resources on the Internet

School of Information, University of Michigan

<http://www.spp.umich.edu/telecom-info.html%OD>

g l o b a l i s s u e s

October 1997 Volume 2 Number 4



Electronic Commerce